İSTANBUL UNIVERSITY CERRAHPAŞA

ORIGINAL ARTICLE
Electrica 2025; 25: 1-13

Cyber-Resilient Frequency Control Design for Interlinked Alternate Current Microgrid System

Dharmesh Kumar[1], Vijay P. Singh[2], Mohammad A. Mallick[1]

[1]Department of Electrical Engineering, Integral University Lucknow, India
[2]Department of Electrical Engineering, Rajkiya Engineering College, Sonbhadra, India

Cite this article as: D. Kumar, V. P. Singh, and M. Mallick, "Cyber-resilient frequency control design for interlinked alternate current microgrid system," *Electrica*, 25, 0002, 2025. doi: 10.5152/electrica.2025.25002.

WHAT IS ALREADY KNOWN ON THIS TOPIC?

- *Interlinked AC microgrids are decentralized power systems that rely on coordinated frequency control to maintain stability, especially due to their low inertia and integration of intermittent renewable sources.*
- *Traditional control strategies like droop and secondary control have been widely studied for frequency regulation.*
- *However, the increasing reliance on communication networks for control and monitoring exposes microgrids to cyber threats such as false data injection and denial-of-service attacks, which can compromise system stability.*
- *To address this, research has progressed toward cyber-resilient control approaches that incorporate secure communication protocols, anomaly detection, and adaptive control strategies.*

***Corresponding Author:** Vijay P. Singh
Email: pratap200697@gmail.com

Received: January 15, 2025
Revision Requested: February 10, 2025
Last Revision Received: February 19, 2025
Accepted: March 5, 2025
Publication Date: June 23, 2025

DOI: 10.5152/electrica.2025.25002

ABSTRACT

In this paper a resilient frequency control design specifically for microgrids (MGs), designed to withstand false data injection attacks (FDIA), is presented. The approach focuses on enhancing the robustness of frequency control mechanisms to ensure stable and reliable microgrid operation, even when subjected to malicious data tampering. The design integrates advanced detection and mitigation strategies to identify and counteract the impact of false data. Initially, the method integrates a bidirectional long short-term memory (BiLSTM) neural network and an improved whale optimization algorithm (IWOA) into a unified framework, working in tandem with a controller to identify and counteract FDIA . Second, a historical MG dataset containing frequency and power variations trains the BiLSTM neural network, enabling it to accurately detect multiple types of FDIAs with high precision. Lastly, the IWOA to the PID (Proportional – Integral – Derivative) controller was applied, effectively counteracting the adverse effects of FDIAs. The results demonstrate that the resilient frequency control system effectively mitigates the adverse effects of FDI attacks, maintaining MG stability and reliability.

Index Terms—Cyber attack, electric vehicles, interlinked microgrid (MG) system, particle swarm optimization algorithm (PSO), renewable energy resources (RESs)

I. INTRODUCTION

The integration of renewable resources and communication infrastructure creates smaller, grid-like networks known as microgrids (MGs) [1]. Educational campuses, hospitals, and military sites are increasingly implementing MGs, and they find extensive use in remote applications such as telecommunications and remote-based households. These MGs utilize advanced metering set-ups for data collection, facilitating the exchange of information via communication networks, which creates a new pattern in energy systems known as cyber-physical microgrids (CPM) [2, 3]. By locally harnessing renewable energy sources (RESs), modern MGs reduce power losses and significantly decrease environmental pollution compared to traditional power systems. Microgrids commonly employ dynamic control, which includes primary, supplementary, and hierarchical control. To react to variations in the MG frequency or the speed of spinning energy sources, primary control comprises the governor or electronic controller quickly adjusting the power output [4]. However, the low inertia and changeable nature of RESs, along with load demand uncertainties, may compromise the effectiveness of primary control. This deterioration may cause an imbalance between supply and demand, leading to frequency variations and even instability. For islanded MGs, which do not receive frequency and voltage support from the main grid, such instability can be disastrous.

Furthermore, a secondary control unit can enhance the primary control response, particularly for energy sources like batteries and EVs (Electric Vehicles) that do not rely on governor-based or droop-based control [5]. Given the variability and uncertainty of non-dispatchable energy resources, extensive energy storage systems are necessary for MGs. Secondary control serves as a supervisory function, leveraging measurements and cyber-communication systems to capture rapid MG dynamics. This significantly enhances the operational reliability of MGs in both

- *The complexity of interlinked microgrids, with their strong cyber-physical interdependencies, further necessitates robust and intelligent designs capable of maintaining operational integrity under cyber-attack scenarios.*

WHAT THIS STUDY ADDS ON THIS TOPIC?

- *This study contributes a novel cyber-resilient frequency control design tailored for interlinked AC microgrid systems, addressing the growing vulnerability of such systems to cyber-attacks.*
- *While traditional control strategies focus primarily on maintaining frequency under normal operating conditions, this research integrates adaptive control logic with real-time anomaly detection to identify and respond to cyber threats such as false data injection and communication disruptions.*
- *The proposed framework enhances system resilience by dynamically adjusting control actions and ensuring stable frequency regulation even during active cyber intrusions.*
- *Through comprehensive simulations under various attack scenarios and interlinked microgrid configurations, the study demonstrates significant improvements in system stability, robustness, and recovery performance compared to conventional approaches.*

grid-connected and islanded modes, surpassing the performance of traditional distribution systems. The swift control response in CPMs can effectively track sudden changes in load and non-dispatchable generation. Using batteries as storage for control is not cost-effective. Instead, EVs operating in vehicle-to-grid mode due to their high availability (around 90% during the day) and low power loss ratio are preferred. Typically, wireless/mobile communication network protocols such as IEEE 802.15.4 (e.g., ZigBee) or IEEE 802.11, which offer more secure communication, are commonly used, discussed in [6]. However, these protocols can compromise security, making data susceptible to manipulation by adversaries.

One form of cyber disruption is denial of service [7], which arises when components of the smart grid become unavailable. The time delay attack, which introduces a delay into communication channels, is another disruptive cyber event [8, 9]. False data injection (FDI) is another type of server attack that occurs when advanced sensors manipulate information [10]. Also, FDI agents make it harder for measurements, control centers, and energy sources to share data in real time. This can cause frequency changes and the wrong defensive protection responses, like cutting off power to generators or load shedding [11]. Such events have significant social and economic repercussions, underscoring the importance of resilient control mechanisms [11], which are crucial for maintaining the normal operations of CPMs. The occurrence of FDI disruptions, as demonstrated by the 2015 Ukraine Blackout events [12], highlights their practical occurrence and the devastating effects they can have. Scholars have explored various methods for detecting FDIin power grids. The authors in [13] discuss the use of a reinforcement learning approach, while authors in [14] and [15] employ risky learning machine techniques. Although these methods are capable of detecting FDI, the state estimation remains static and non-dynamic in [16]. To detect fraudulent data introduced into power systems, a detection framework based on artificial neural networks and Kalman filters is provided in [17, 18]. Given that not all system states can be directly observed due to financial restrictions [19–21]. Further authors of [22, 23] presented state estimators and observers to detect attacks in smart grids. These approaches avoid the curse of dimensionality and seem plausible. However, the measurements and system states are constantly perturbed by uncertainties arising from RESs and disturbances from FDIs, which renders them inappropriate for direct use in feedback control. Although Kalman filters are frequently employed for state estimation, threshold settings may have an impact on their accuracy [24]. Conventional Leuenberger observers cannot distinguish between signals and treat ambiguous signals in the same way [25]. Although they provide an alternative, sliding-mode observers are vulnerable to excessive chattering [26]. A model-based method for estimating and identifying unknown inputs was presented by the authors [27, 28], but they did not concentrate on managing or averting disruptions. This paper develops an optimal controller for an islanded MG based on Unknown Input Observer (UIO). This controller may identify uncertainties and FDI and then mitigate them without depending on a predetermined threshold. Current detection and defense methods have certain limitations, which can be categorized as follows:

1. Limited Scope and Generality: Some researchers focus on a narrow range of false data injection attacks (FDIAs) and propose detection methods without implementing corresponding defense strategies. It is important to develop detection and defense measures that are applicable across diverse types of FDIAs.
2. Dependency on System Parameters: Model-based methods for detection and defense rely heavily on the parameters of MGs. For instance, strategies presented in [29] require precise estimation of the system state, which may not always be feasible for real-world applications.
3. Increased System Overhead: Certain defense approaches, such as bandwidth allocation and event-triggered algorithms can add significant overhead and complexity to the system.
4. Further research is required to evaluate the effectiveness of current detection and defense methods, particularly when addressing multiple FDIAs simultaneously in interlinked AC MG.

This paper's primary major contribution is as follows.

- To successfully identify and reduce the negative impacts of the three different types of FDIAs such as step, pulse, and random. For this a unique detection and defense mechanism has been devised.
- Since both past and future states have an impact on the current state of the MG system, a detection technique based on the bidirectional long short-term memory (BiLSTM) neural network has been introduced in this study. The three FDIA kinds can be accurately detected by

this method, which efficiently gathers information from both past and future sequences.
- After the BiLSTM identifies an FDIA, a defense technique has been developed that uses the IWOA to improve the PID controller parameters in the distributed LFC (Load Frequency Control) system. System stability is maintained by this optimization, which guarantees that the PID controller maintains frequency deviations within the typical range. Further, dynamic performance of system has been compared with other methods available in literature.

The following is the arrangement of the remaining sections of the paper: In Section II, the interconnected MG system which includes many generating sources is mathematically modeled. The detection and defensive mechanism for FDIA control was proposed in Section III. Section IV, presents the simulation results and remarks of the proposed controller. The paper's conclusion is given in Section V.

II. MATHEMATICAL MODELLING

The schematic of MG system over communication network is depicted in Fig. 1, which consists of distributed generation and load. A distributed management system (DMS) at control center of interlinked AC MG obtain the required state information through measurements of signals. The DMS also communicates decisions and logic processing to the actuators of energy sources, such as the DG and EV stations, thereby establishing a cyber-infrastructure for the CPM.

A. State Space Modeling of Microgrid

The state space modeling of an interlined AC MG system is given in (1–2)

$$\dot{x}(t) = Ax(t) + Bu(t) + Dd(t) \tag{1}$$

$$y(t) = Cx(t) \tag{2}$$

Where, $x(t)$ denotes the state vector of MG $x(t) = \left[\Delta f \quad \Delta P_g \quad \Delta P_{WG} \quad \Delta P_{EV} \quad \Delta P_{PV} \quad \Delta P_{ESS}\right]^T$, $u(t)$ represents the input control of MG, $d(t)$ represents the unknown disturbance to MG System. A is the state matrix, B, C, D are input matrix, output matrix and load perturbation of studied MG system respectively. The matrices are given in (3–9) as follows.

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \tag{3}$$

$$A_{11} = \begin{bmatrix} \frac{-D}{H} & \frac{-1}{H} & 0 & \frac{-1}{H} & \frac{-1}{H} & 0 \\ 0 & \frac{-1}{T_t} & \frac{1}{T_t} & 0 & 0 & 0 \\ 0 & 0 & \frac{-1}{T_{PV}} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{-1}{T_{WT}} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{-1}{T_{EV}} & \frac{1}{T_{EV}} \\ \frac{-1}{R_i T_G} & 0 & 0 & 0 & 0 & \frac{-1}{T_G} \end{bmatrix} \tag{4}$$

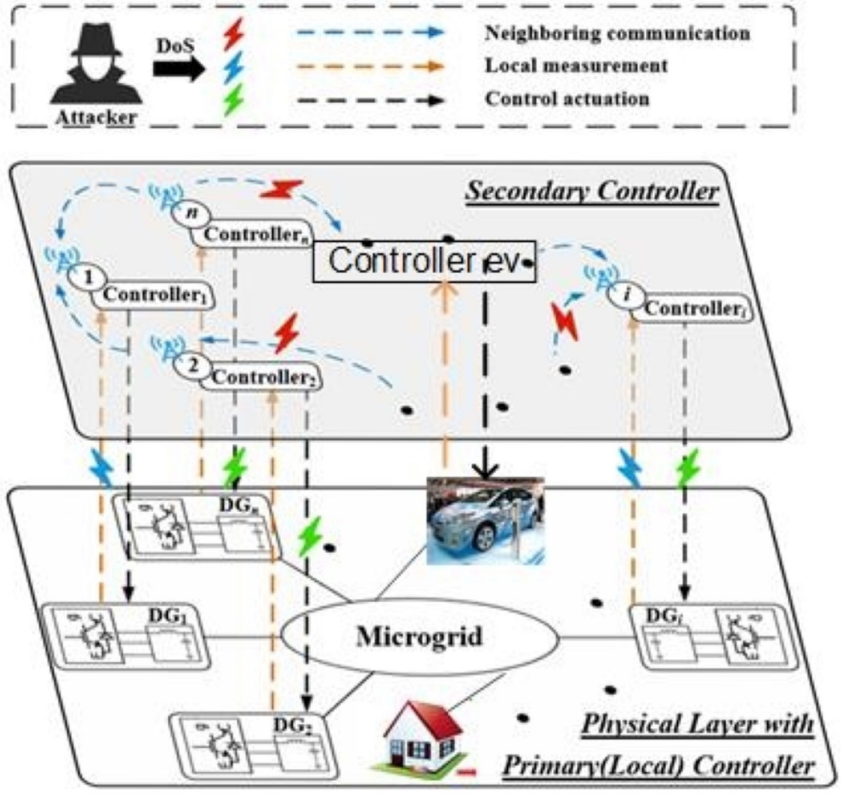

Fig. 1. Schematic of microgrind system under attack.

$$A_{12}=\begin{bmatrix} \frac{-1}{H} & 0 & 0 & \frac{-1}{H} & \frac{-1}{H} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (5)$$

$$A_{22}=\begin{bmatrix} \frac{-1}{T_{EV}} & \frac{1}{T_{EV}} & 0 & 0 & 0 \\ 0 & \frac{-1}{T_{PV}} & \frac{1}{T_{PV}} & 0 & 0 \\ 0 & 0 & \frac{-1}{T_G} & 0 & 0 \\ 0 & 0 & 0 & \frac{-1}{T_{WT}} & 0 \\ 0 & 0 & 0 & 0 & \frac{-1}{T_{\beta G}} \end{bmatrix} \quad (6)$$

$$B=\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & \frac{1}{T_G} & 0 & 0 & \frac{1}{T_{WT}} & 0 & 0 \end{bmatrix}^T \quad (7)$$

$$C=\begin{bmatrix} \frac{-1}{H} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{T_{WT}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^T \quad (8)$$

$$D=\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^T \quad (9)$$

B. False Data Injection Attacks on Interlinked Alternate Current Microgrid

The LFC controller uses data from the frequency deviation to control the MG, and the security of this data is essential to the correct operation of the control commands in the LFC system. As illustrated in Fig. 2, a cyberattack can infiltrate the frequency deviation channel, concealing itself from the LFC controller and appearing identical to the initial system state vector. Equation (10) describes how the BDD (Bad Data Detection) system in the distributed LFC system uses a residual test to detect FDIAs.

$$\begin{cases} p_a = p + a \\ x_a = x + c \\ p_a - Jx_{a2} = (p - Jx) + (a - JC)_2 \le p - Jx_2 \\ a - Jc_2 \le \mu \end{cases} \quad (10)$$

Here, p_a represents the state variable with FDIAs, a is the injected attack vector, p is the state variable, c denotes the deviation from normal system states x_a, μ is the threshold pre-set by the BDD system, and J is the Jacobian matrix of the power system. If the attack vector fulfills the requirement conditions in (11), the FDIA can successfully inject manipulated data into the power system without being detected by the BDD system's residual test. In this paper, all constructed FDIAs satisfy the conditions in (11).

$$\begin{cases} a = Jc \\ a - Jc_2 \le \mu - p - Jx_2 \end{cases} \quad (11)$$

Further, the study covers three types of FDIAs, including pulse, step, and random attacks in this study.

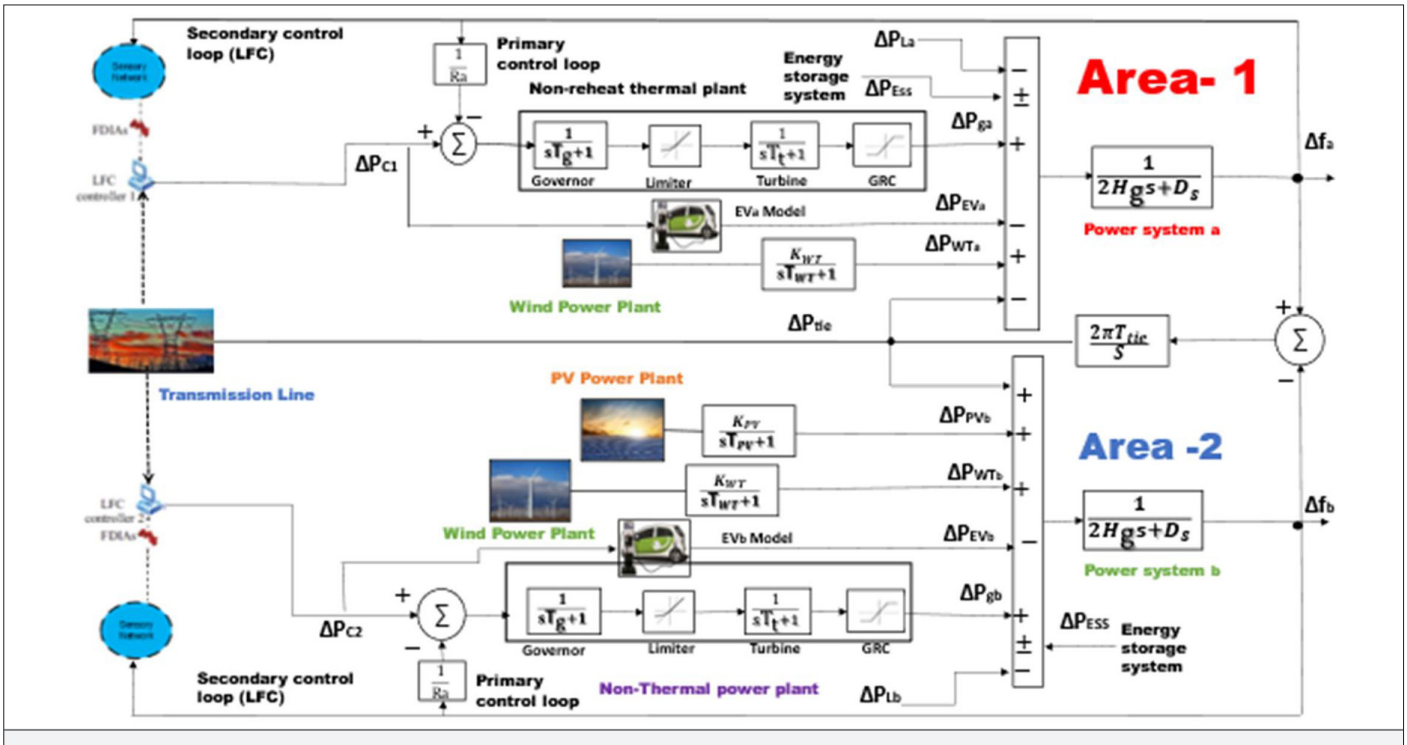

Fig. 2. Two area interconnected microgrid system with false data injection attacks.

1) Pulse Attack: (A_p)

The attacker introduces false data Δf_a in the form of pulses over a period of time in actual signal, represented as:

$$f_a(t) = \{\Delta f_{a1} \quad t\ \varepsilon[t_{ia} \quad t_{fa}], 0 otherwise \tag{12}$$

2) Step Attack: (As)

In this type of attack from starting at a predefined time, the attacker continuously injects false data Δfa_2 into the LFC system, represented as:

$$f_a(t) = \begin{cases} 0 & t < t_{ia} \\ \Delta f_{a2} & t \geq t_{ia} \end{cases} \tag{13}$$

3) Random Attack: (A_r)

In this type of attack at random times, the attacker injects a false data Δf_{a3}, such as sinusoidal, random, etc. in original signal, can be expressed as:

$$f_a(t) = \Delta f_{a3} \tag{14}$$

III. DETECTION AND DEFENSE MECHANISM FOR INTERLINKED ALTERNATE CURRENT MICROGRID

This section presents the proposed detection and defense method. The BiLSTM neural network is capable of detecting three types of FDIAs outlined in this paper, while the improved whale optimization algorithm (IWOA) optimizes the PID controller parameters to keep the frequency response of system within the required limit.

A. Detection Using Bidirectional Long Short-term Memory Neural Network

A sophisticated kind of recurrent neural network (RNN), the long short-term memory (LSTM) neural network was created to solve the vanishing gradient issue that conventional RNNs frequently face. The vanishing gradient problem in deep networks makes it challenging to efficiently update weights during backpropagation, especially for earlier time steps, as the model rapidly loses knowledge over time. This issue, sometimes referred to as the "Long-term dependency problem," restricts the model's capacity to efficiently extract data from earlier occurrences.

Researchers all across the world have altered RNN models to address this, with the LSTM neural network emerging as the most well-known method. In contrast to conventional RNNs, LSTM networks add a special four-layer repeating module while maintaining the chain structure. This structure supports long-term memory and enhances model efficacy by allowing LSTM networks to selectively preserve important information while discarding less pertinent input. The fundamental design of a BiLSTM neural network, which has a two-way cyclic architecture with both forward and backward propagation, is shown in Fig. 3. The output of the model is represented by y, and the hidden layers for the past and future contexts function independently of one another.

$$\begin{cases} \overrightarrow{h_t} = L\left(x_t \quad \overrightarrow{h_{t-1}}\right) \\ \overleftarrow{h_t} = L\left(x_t \quad \overleftarrow{h_{t-1}}\right) \end{cases} \tag{15}$$

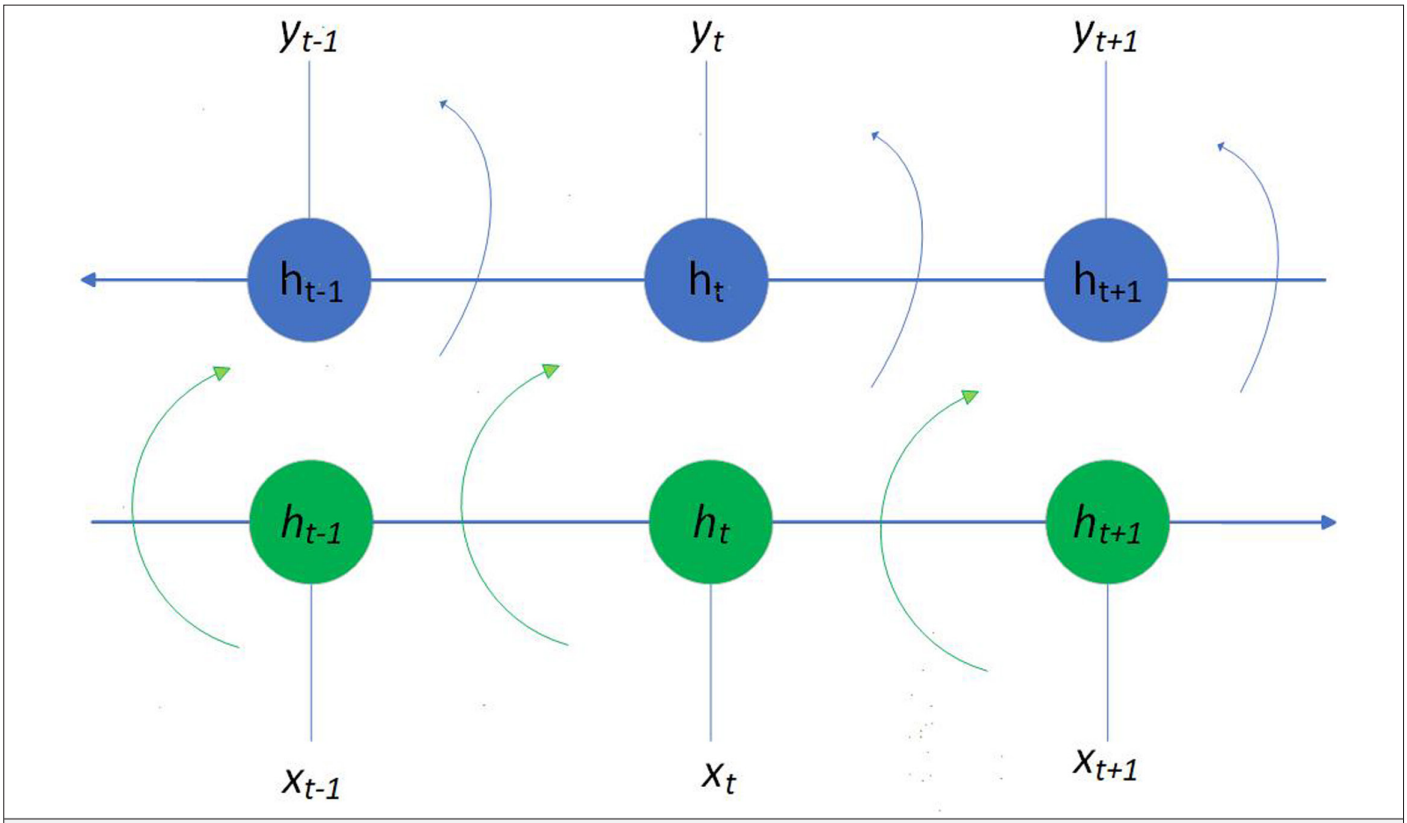

Fig. 3. Basic structure of bidirectional long short-term memory neural Network.

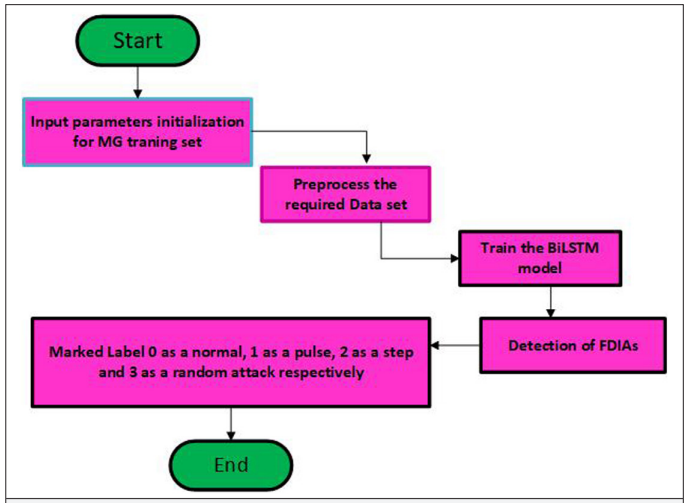

Fig. 4. Bidirectional long short-term memory detection process.

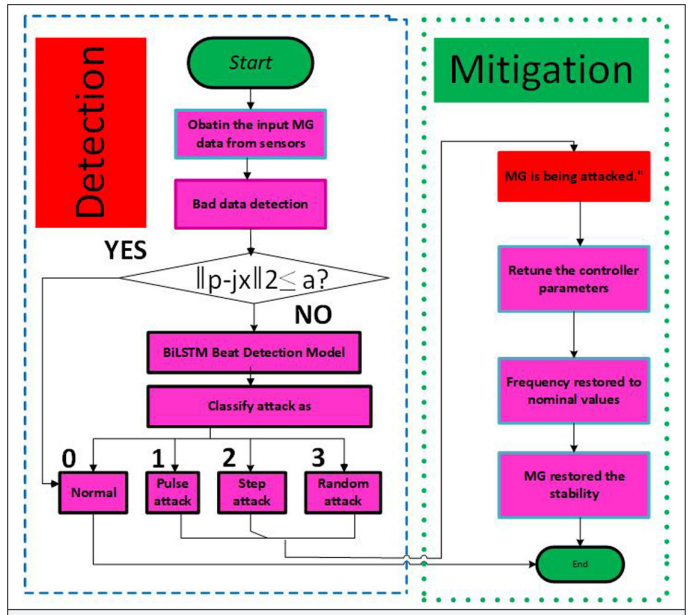

Fig. 5. Flowchart of detection and defense mechanism.

In this context, $\overleftarrow{h_t}$ represents the hidden layer state of the forward LSTM neural network at time *t*, and $\overrightarrow{h_t}$ denotes the hidden layer state of the reverse LSTM neural network at the same time *t* and *L* refers to the LSTM cell. The complete hidden layer state of the network, h_t, is obtained by combining $\overleftarrow{h_t}$ and $\overrightarrow{h_t}$. The BiLSTM network constructs three different types of FDIA in four labels, as shown in Fig. 4. To train the BiLSTM model and evaluate its performance on a separate test set processed dataset was used. The trained model was implemented to mitigate FDIAs in the distributed load frequency control (LFC) system of the MG.

B. Microgrid with Detection and Defense Mechanism

In this study, the advanced capabilities of BiLSTM neural networks and IWOA to detect and mitigate FDIAs in MGs are utilized. This approach integrates a BiLSTM neural network and IWOA into a decentralized LFC system to analyze and prevent FDIAs within distributed LFC data. By applying this method, the MG's frequency deviation within an acceptable error range is maintained, ensuring its security and stability. Fig. 5 illustrates the LFC system with its detection and defense mechanisms, embedded within the LFC controller framework. Here, trained BiLSTM networks analyze input data to flag potential threats. Upon identifying an FDIA, IWOA is immediately triggered to optimize PID controller parameters, countering any frequency deviations caused by the attack. When the primary MG faces an FDIA, the LFC controller typically responds to frequency deviation data, though this response may involve a time delay and may not adequately protect MG security. The proposed method addresses these limitations, offering a robust method of detection and defense mechanisms that enhance MG security. Through prompt FDIA detection and optimized PID controller settings, the BiLSTM and IWOA provide high detection accuracy and defense strength, bolstering MG stability and preventing FDIAs. Importantly, this detection and defense mechanism activates specifically in the presence of FDIAs, leaving MG's normal operations unaffected. It can be seamlessly integrated with existing LFC controllers, requiring minimal investment and showcasing excellent scalability without additional protection measures.

Inspired by the way whales prey, the whale optimization algorithm (WOA) is a new intelligent optimization technique. One of its benefits is that it requires less parameters, enhanced accuracy, and quicker convergence. Each whale location in WOA represents a target solution, and the algorithm uses three different approaches to update the positions in order to find the best solution: random search, spiral search, and encircling prey [29]. An enhanced version known as the IWOA is suggested in order to achieve a balance between local and global search capabilities. By adding a nonlinear convergence factor, the IWOA improves its capacity to manage intricate, large-scale optimization issues in the MG. The IWOA efficiently synchronizes local and global search capabilities, lowering the chance of converging to a local optimum by applying a diversity variation operation to the currently optimal whale individuals and varying the convergence factor non-linearly with the number of evolutionary selections [29]. This study proposes the IWOA as a defense against FDIAs to solve the volatility of the LFC system under FDIAs. When the BiLSTM detection model sends signals, IWOA quickly adjusts the PID controller settings in the LFC system. By using its strong local and global search capabilities, IWOA can determine the ideal PID settings, allowing the controller to mitigate the effects of FDIA and improve the LFC system's resilience and security.

IV. SIMULATION RESULTS AND ANALYSIS

This subsection demonstrates the effectiveness of the Proposed Method for Detection and Defense Against FDIAs in the MG. The MG simulation model is shown in Fig. 2, with simulations conducted using MATLAB/Simulink. Further, between 10 and 40 seconds, the load demand progressively drops to 0.5 p.u. after rising to 0.9 p.u. in the first 10 seconds. Finally, the load remains 0.5 p.u. between 40 and 50 seconds. The parameters for the two-area interconnected MG are detailed in [30].

A. Analysis of Detection/Defense Method

The model is trained over 100 epochs and has 100 hidden units is given in Table 1. It takes about 34 minutes to train the BiLSTM neural network. The BiLSTM network does not use the system's computational resources while operating because it is trained offline. To aid in convergence toward an ideal solution, the learning rate is first set

TABLE I. BIDIRECTIONAL LONG SHORT-TERM MEMORY NEURAL NETWORK PARAMETERS

Parameters	Value
Input Size	1
Total no. of classes	4
No. of hidden units	100
Total Epoch	100
Threshold value	1
Learning rate	0.005
Learning rate drop period	125
Learning rate drop factor	0.2

at 0.005 for the first 50 epochs and subsequently lowered by a decay factor of 0.2. Furthermore, Fig. 6 shows the BiLSTM network's training accuracy and loss following 100 epochs. With a training accuracy of around 98% and a training loss of less than 0.5 throughout, the graph demonstrates the model's remarkable performance. With an accuracy of 0.98972 and an F1-score of 0.97357, the BiLSTM detection model presented in this research outperforms the other models in all four metrics shown in Table II. This demonstrates how much better the BiLSTM model is at identifying FDIAs. The BiLSTM model exhibits a definite advantage over other benchmark models, such as SVM (Support Vector Machine), LSTM, and LSTM-attention. Among these models, the BiLSTM performs significantly better than its peers, as seen by the second-highest F1-score of 0.8812. These outcomes confirm the remarkable efficacy and capability of the BiLSTM model in identifying FDIAs.

The purpose of this study was to assess the efficacy of the suggested defense and detection strategy for three different kinds of FDIAs, each of which targets the frequency signal in particular. The first attack, which starts at t = 10 seconds and has an attack magnitude

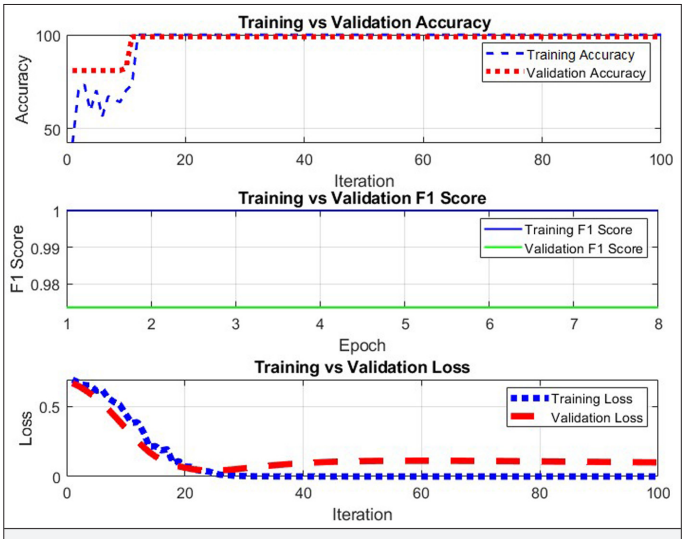

Fig. 6. Bidirectional long short-term memory neural network training accuracy, F1 score and loss.

TABLE II. DETECTION PERFORMANCE OF VARIOUS MODEL

Model	Accuracy	Precision	F-Score	Recall
BiLSTM	0.9897	0.9485	0.97357	0.9171
LSTM	0.9041	0.8812	0.8421	0.8312
LSTM-attention	0.9315	0.9121	0.8752	0.8812
SVM	0.7952	0.7562	0.7152	0.6932

BILSTM, bidirectional long short-term memory; LSTM, long short-term memory; SVM, Support Vector Machine.

of 0.8 p.u., is regarded as a pulse attack in which FDIA hits the LFC system. Moreover, the second attack is a phase in which FDIA uses a 0.2 p.u. magnitude attack level to target the LFC system at t = 10 seconds. The third attack type, random attack, incorporates both random and sinusoidal components in FDIA. Beginning at t = 0 seconds, the random component introduces attack magnitude into the LFC system with values between 0.095 and 0.115 p.u. Additionally, simulation results have been performed for the sinusoidal FDIA component, which injects FDIA magnitude into the system within a range of 0.15 p.u. starting at t = 0.

Figs. 7-9 depict the three different kinds of FDIAs. Unlike the PID controller optimized by IWOA, the original PID controller cannot rectify frequency discrepancies as the load varies, as seen in Figs. 10-13. Frequency variations under the original PID controller can be as much as 0.03 p.u. Nonetheless, the frequency variation is minimal and stays well within the allowable error range when the PID controller is optimized by IWOA.

Improved whale optimization algorithm's performance is assessed by contrasting it with two alternative control strategies, namely particle swarm optimization (PSO) and WOA. When working with the three types of FDIAs, the PID parameters optimized by WOA and PSO produce oscillations that beyond the allowable error range, failing to maintain frequency stability, as illustrated in Figs. 10-13. It is clear that, IWOA successfully removes the frequency deviation brought on

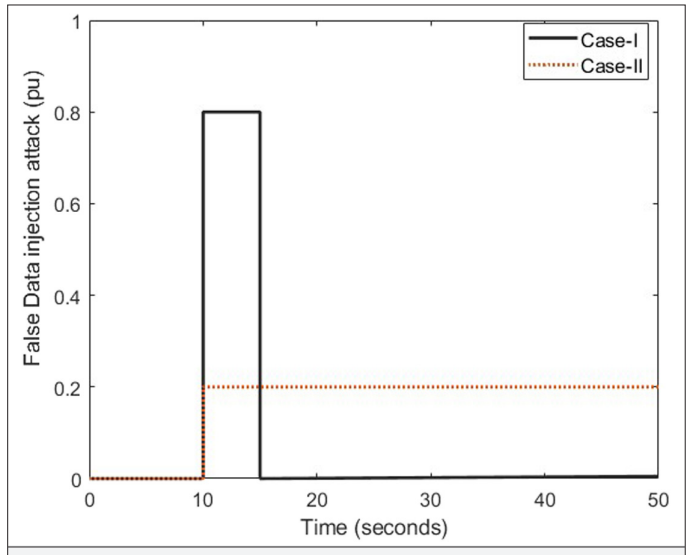

Fig. 7. First and second type of false data injection attack.

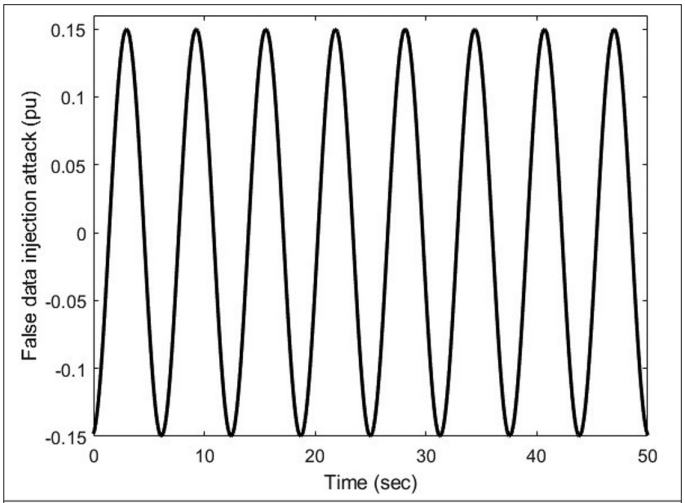

Fig. 8. Third type of false data injection attack as a sinusoidal form.

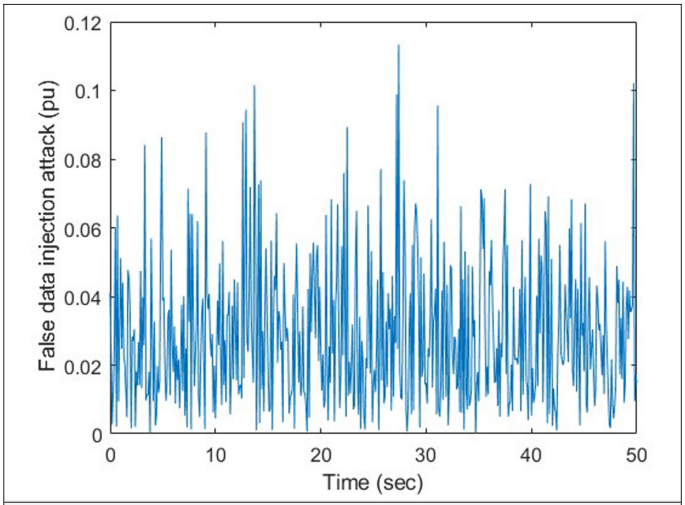

Fig. 9. Third type of false data injection attack as a random form.

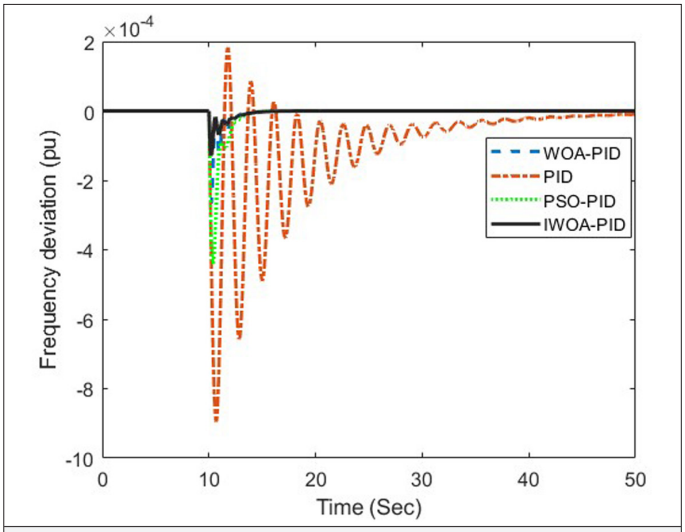

Fig. 10. Frequency deviation area-1 for first type of false data injection attack control.

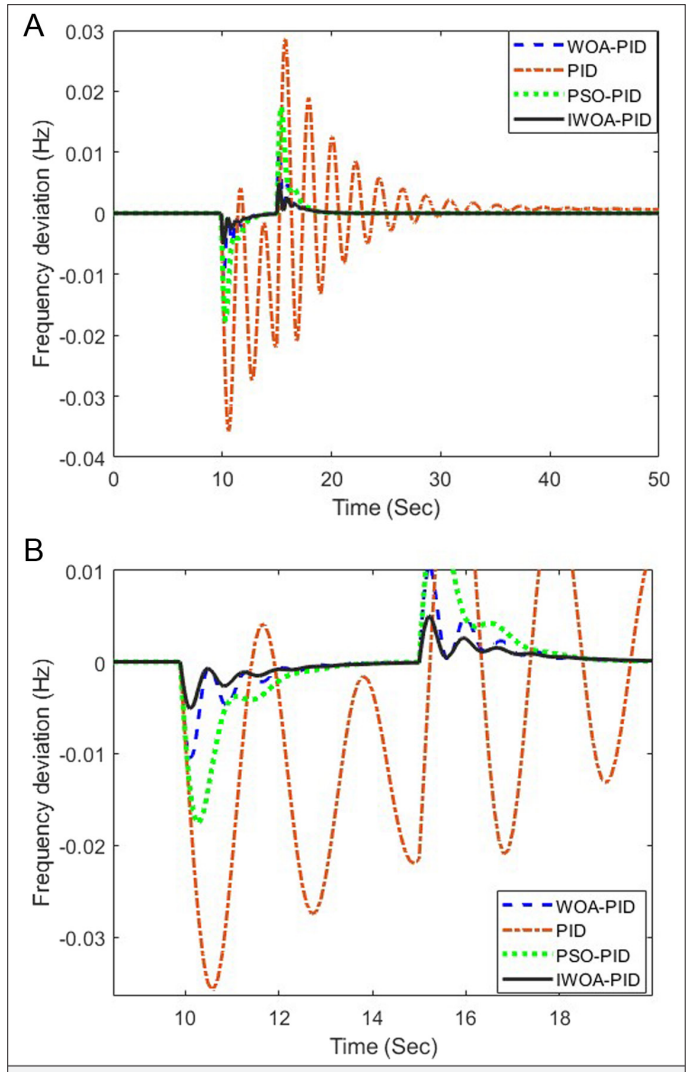

Fig. 11. (a) Frequency deviation of second type of false data injection attack control—area-1. (b) Zoom plot of frequency deviation of second type of false data injection attack control—area-1.

by FDIAs, maintaining the frequency within the typical error range and guaranteeing system stability. These results demonstrate that IWOA is superior to other optimization algorithms in reducing the negative impact of FDIAs on frequency stability.

B. Case-1 (Pulse-type False Data Injection Attack)

At t =10 seconds, the attacker injects a pulse-type FDIA and introduces erroneous data into the MG. The MG is in an unstable state when it is controlled by the original PID controller because it exhibits a large frequency deviation at t = 10 seconds that approaches 01 p.u. On the other hand, the MG rapidly corrects the frequency deviation to zero when it is controlled by the PID controller optimized using IWOA. This occurs at t =10 seconds. As seen in Fig. 10, the MG system is at steady for the next 40 seconds. This indicates that pulse-type FDIAs are successfully countered and system stability is maintained by the PID controller optimized using IWOA as compared to other optimization method such as WOA-PID, PSO-PID, and PID. The proposed method is superior in terms of settling time, undershoot etc. and therefore maintain the stability of system and less prone to FIDA.

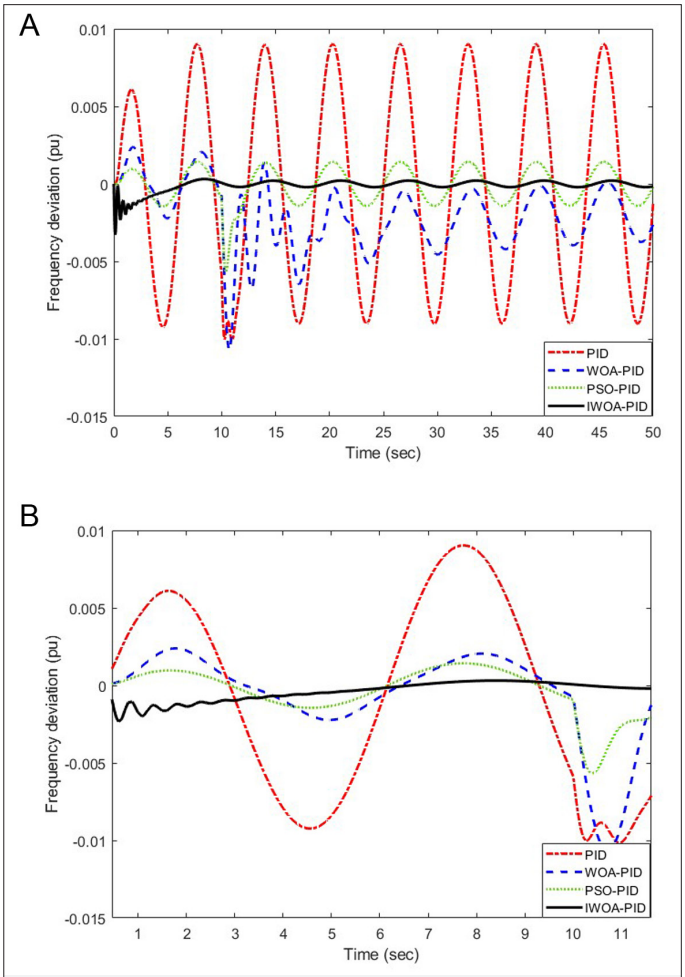

Fig. 12. (a) Frequency deviation of sinusoidal false data injection attack control. (b) Zoom plot of Frequency deviation of sinusoidal false data injection attack control.

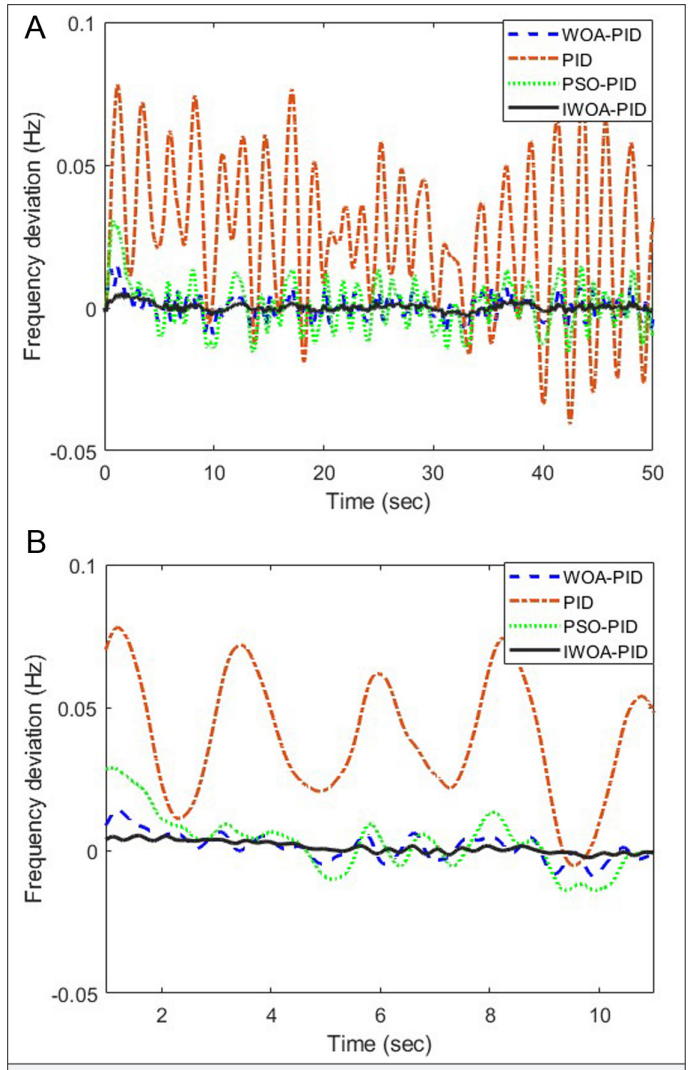

Fig. 13. (a) Frequency deviation of random false data injection attack control. (b) Zoom plot of Frequency deviation of random false data injection attack control.

C. Case-2 (Step type False Data Injection Attack)

From Fig. 11, the attacker continuously introduces erroneous data into the system at $t = 10$ seconds in the second form of FDIA. The stability of the MG controlled by the typical PID controller is seriously disrupted within the first 5 seconds by large frequency fluctuations, as seen in Fig. 11(a). The zoom plot of frequency deviation of second type of FDIA control for area-1 is given in Fig. 11(b). Further, the attack significantly weakens the MG's stability at $t = 10$ seconds, resulting in a frequency variation of −0.09 p.u., or nearly −0.1 p.u. After identifying the FDIA in the MG, the BiLSTM neural network sends a defense signal to the IWOA. The IWOA-optimized PID controller then quickly recalculates the ideal PID parameters in a defensive move. This guarantees stability throughout the attack by enabling the system to keep the frequency variation within the allowable error tolerance. These findings demonstrate that, in step-type FDIA settings, the suggested PID controller improved by IWOA successfully preserves MG stability.

D. *Case-3 (Random Type False Data Injection Attack)*

The third kind of attack targets the LFC system by combining random and sine signals in the attack vector, as shown in Figs. 8 and 9 have been applied to the system. Fig. 12(a) shows the frequency deviation of sinusoidal FDIA control and its zoom plot is given in Fig. 12(b). Further, Fig. 13(a) shows frequency deviation of random FDIA control. And its zoom plot is given in Fig. 13(b). The system is more severely affected by this kind of FDIA than by the other two of attack. This attack is too strong for the LFC system managed by the conventional PID controller, resulting in long-lasting, significant frequency oscillations. The frequency deviation varies between 0.12 and 0.05 p.u. under the random signal and between 0.06 and.05 p.u. under the sine signal. The stability of the MG is seriously threatened by these oscillations, which last for 50 seconds. Further, the control area of both area is shown in Fig. 14. The tie-line power deviation is shown in Fig. 15. The active power deviation of area-1 and area-2 is shown in Fig. 16(a) and 16(b) respectively. It is evident from the data that the IWOA-based protection mechanism that was suggested in this study reacts rapidly to a defense signal from the BiLSTM. The MG's frequency stability is essentially maintained since the adjusted frequency deviation is completely within the permitted error range, even in the face of random FDIA attacks. This efficiently maintains the system in a stable zone and guarantees the mitigation of FDIA.

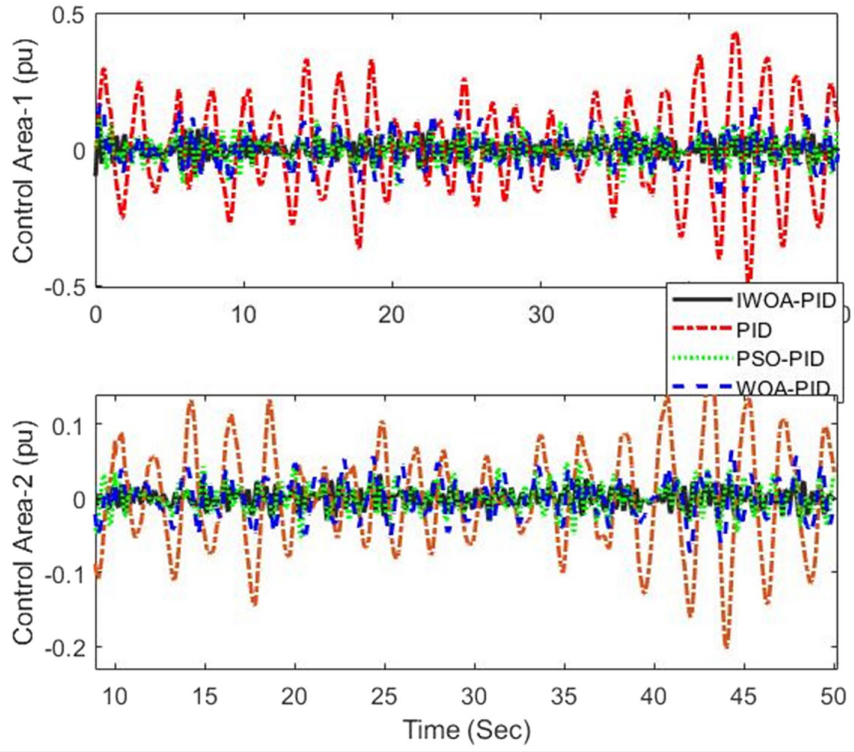

Fig. 14. Control signal for both areas.

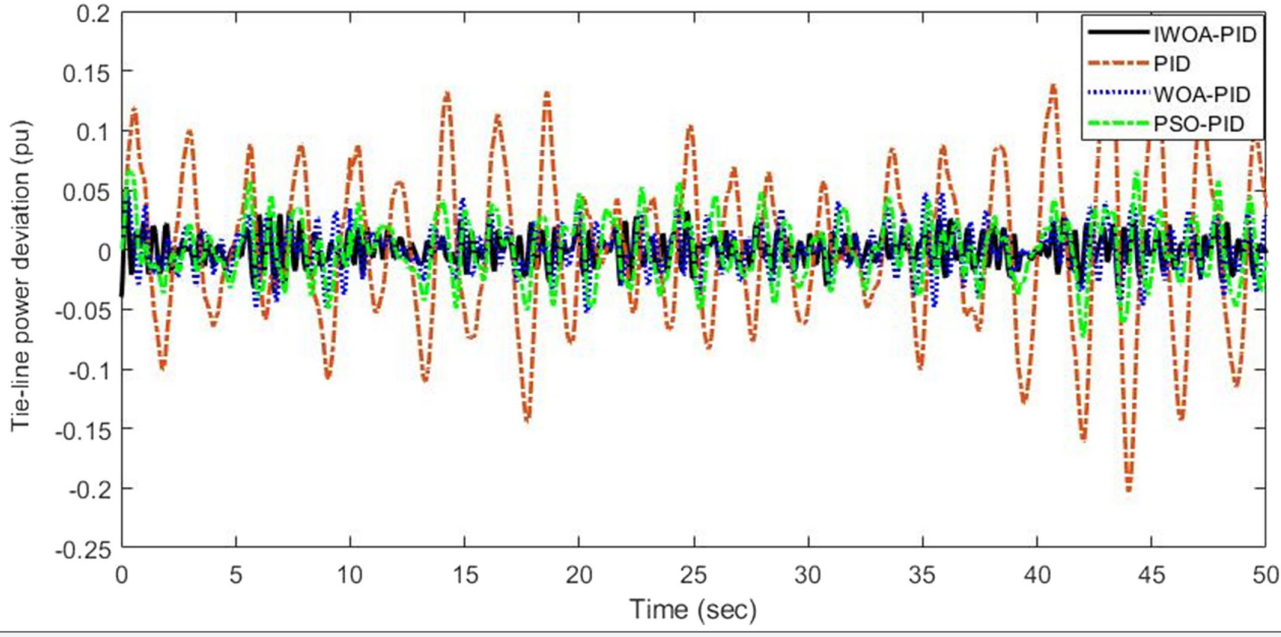

Fig. 15. Tie-line power deviation.

V. CONCLUSION

This paper focuses on developing detection and defense techniques to address FDIAs in interlinked AC MG systems. In this study firstly, a detection and defense model are integrated into the LFC controller to identify and mitigate the adverse effects of FDIAs. The offline-trained BiLSTM neural network powers the detection process, and simulation results validate its accuracy. The defense strategy also uses the IWOA to fine tune the PID controller parameters. This keeps system frequency deviations within the acceptable range and the microgridMG stable even when FDIA is present. The obtained results have also been compared with other existing methods. Simulation results confirm the proposed method's effectiveness in countering various types of FDIAs and preserving MG stability. Future, research

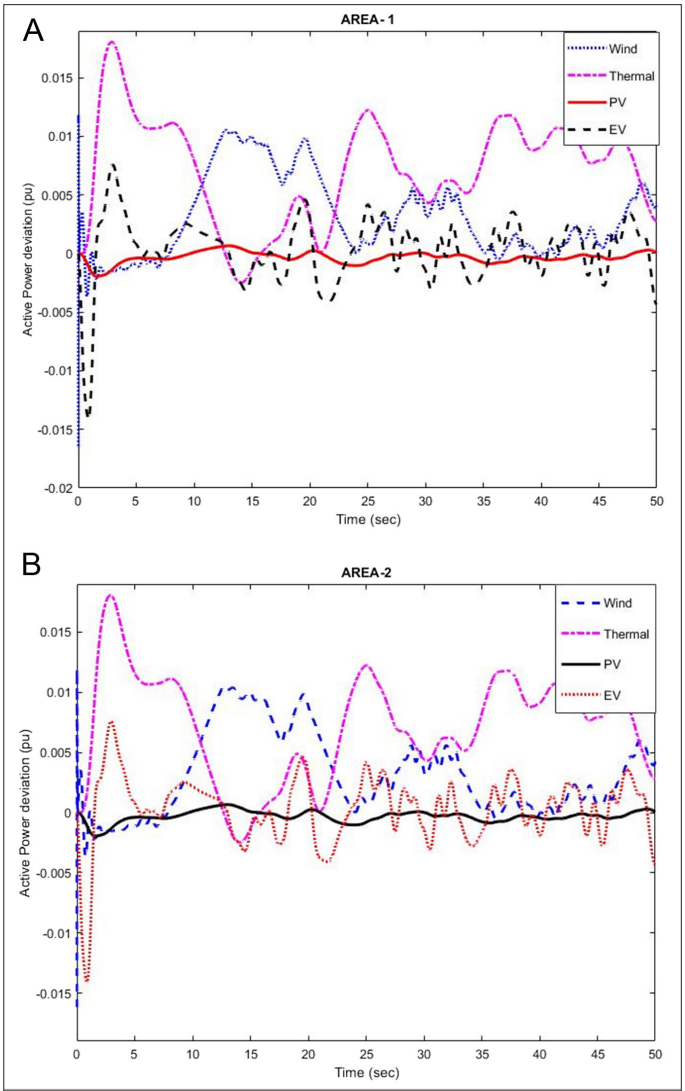

Fig. 16. (a) Active power deviation area-1. (b) Active power deviation area-2.

will explore defense mechanisms against adversarial machine learning attacks in MGs.

Data Availability Statement: The data that support the findings of this study are available on request from the corresponding author.

Peer-review: Externally peer reviewed.

Acknowledgment: Thanks to Integral University, Lucknow for providing manuscript communication number IU/R&D/2025-MCN0003346 and necessary support for the research.

Author Contributions : Concept – D.K., V.P.S.; Design – D.K., V.P.S; Supervision – M.A.M., V.P.S.; Resources – D.K., M.A.M.; Materials – D.K.; Data Collection and/or Processing – D.K., V.P.S.; Analysis and/or Interpretation – D.K., M.A.M.; Literature Search – D.K.; Writing – D.K., V.P.S.; Critical Review – M.A.M., V.P.S.

Declaration of Interests : The authors have no conflicts of interest to declare.

Funding: The authors declared that this study received no financial support.

REFERENCES

1. B. Zhou *et al.*, "Multi-microgrid energy management systems: Architecture, communication, and scheduling strategies," *J. Mod. Power Syst. Clean Energy*, vol. 9, no. 3, pp. 463–476, 2021. [CrossRef]
2. T. Adefarati, and R. C. Bansal, "Reliability, economic and environmental analysis of a microgrid system in the presence of renewable energy resources," *Appl. Energy*, vol. 236, pp. 1089–1114, 2019. [CrossRef]
3. A. F. Minai *et al.*, "Evolution and role of virtual power plants: Market strategy with integration of renewable based microgrids," *Energy Strategy Rev.*, vol. 53, 2024. [CrossRef]
4. K. K. Bharti, V. P. Singh, and S. P. Singh, "Impact of intelligent demand response for load frequency control in smart grid perspective," *IETE J. Res.* Taylor Francis, 2020.
5. D. Du *et al.*, "A review on cybersecurity analysis, attack detection, and attack defense methods in cyber-physical power systems," *J. Mod. Power Syst. Clean Energy*, vol.11, no. 3, pp. 727–743, 2023. [CrossRef]
6. Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "A cyber-attack resilient distributed control strategy in islanded microgrids," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 3690–3701, 2020. [CrossRef]
7. D. Liu, A. Dyśko, Q. Hong, D. Tzelepis, and C. D. Booth, "Transient wavelet energy-based protection scheme for inverter-dominated microgrid," *IEEE Trans. Smart Grid*, vol. 13, no. 4, pp. 2533–2546, 2022. [CrossRef]
8. R. Jiao, G. Xun, X. Liu, and G. Yan, "A new AC false data injection attack method without network information," *IEEE Trans. Smart Grid*, vol. 12, no. 6, pp. 5280–5289, 2021. [CrossRef]
9. A. S. Mohamed, M. F. M. Arani, A. A. Jahromi, and D. Kundur, "False data injection attacks against synchronization systems in microgrids," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4471–4483, 2021. [CrossRef]
10. S. Xu, Y. Qian, and R. Q. Hu, "On reliability of smart grid neighborhood area networks," *IEEE Access*, vol. 3, pp. 2352–2365, 2015. [CrossRef]
11. R. Tan et al., "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Trans. Inf. Forensics Sec.*, vol. 12, no. 7, pp. 1609–1624, 2017. [CrossRef]
12. G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, 2017. [CrossRef]
13. Y. Chen, S. Huang, F. Liu, Z.Wang, and X. Sun, "Evaluation of reinforcement learning based false data injection attack to automatic voltage control," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2158–2169, 2019. [CrossRef]
14. L. Yang, Y. Li, and Z. Li, "Improved-elm method for detecting false data attack in smart grid," *Int. J. Electr. Power Energy Syst.*, vol. 91, pp. 183–191, 2017. [CrossRef]
15. D. Xue, X. Jing, and H. Liu, "Detection of false data injection attacks in smart grid utilizing elm-based ocon framework," *IEEE Access*, vol. 7, pp. 31762–31773, 2019. [CrossRef]
16. A. Farraj, E. Hammad, and D. Kundur, "On the impact of cyber-attacks on data integrity in storage-based transient stability control," *IEEE Trans. Ind. Inform.*, vol. 13, no. 6, pp. 3322–3333, 2017. [CrossRef]
17. J. Zhao, L. Mili, and M. Wang, "A generalized false data injection attacks against power system nonlinear state estimator and countermeasures," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4868–4877, 2018. [CrossRef]
18. S. K. Tripathi, V. P. Singh, R. K. Patel, and A. S. Pandey, "Impact of Different types of Cyber-Physical Attack and its Prevention on Load Frequency Control," 15th International Conference on Computational Intelligence and Communication Networks (CICN), Bangkok, Thailand. New York: IEEE, 2023, pp. 410–414. [CrossRef]
19. Y. Li, H. Fang, and J. Chen, "Anomaly detection and identification for multiagent systems subjected to physical faults and cyber attacks," *IEEE Trans. Ind. Electron.*, vol. 67, no. 11, pp. 9724–9733, 2020. [CrossRef]
20. X.Yang, P. Zhao,X.Zhang, J. Lin, andW. Yu., "Toward a Gaussian-mixture model-based detection scheme against data integrity attacks in the smart grid," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 147–161, 2017
21. X.Wang, X. Luo, M. Zhang, and X. Guan, "Distributed detection and isolation of false data injection attacks in smart grids via nonlinear unknown input observers," *Int. J. Electr. Power Energy Syst.*, vol. 110, pp. 208–222, 2019. [CrossRef]

22. M. R. Khalghani, J. Solanki, S. Khushalani-Solanki, and A. Sargolzaei, "Stochastic load frequency control of microgrids including wind source based on identification method," in *Proc. Environ. Electr. Eng. IEEE Ind. Commercial Power Syst. Eur.* New York: IEEE, 2018, pp. 1–6. [CrossRef]
23. M. A. Siddiqui, M. N. Anwar, and S. H. Laskar, "Sliding mode controller design for second-order unstable processes with dead-time," *J. Electr. Eng.*, vol. 71, no. 4, pp. 237–245, 2020. [CrossRef]
24. M. A. Siddiqui, M. N. Anwar, S. H. Laskar, and M. R. Mahboob, "A unified approach to design controller in cascade control structure for unstable, integrating and stable processes," *ISA Trans.*, pp. 1–16, 2020.
25. S. Prasad, S. Purwar, and N. Kishor, "Non-linear sliding mode-based load frequency control for power systems using unknown-input-observer," in *Proc. Control Conf.* New York: IEEE, 2017, pp. 233–239. [CrossRef]
26. A. F. Taha, A. Elmahdi, J. H. Panchal, and D. Sun, "Unknown input observer design and analysis for networked control systems," *Int. J. Control*, vol. 88, no. 5, pp. 1–15, 2015. [CrossRef]
27. A. Ameli, A. Hooshyar, E. F. El-Saadany, and A. M. Youssef, "Attack detection and identification for automatic generation control systems," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4760–4774, 2018. [CrossRef]
28. S. M. Bozorgi, and S. Yazdani, "IWOA: An improved whale optimization algorithm for optimization problems," *J. Comp. Des. Eng.*, vol. 6, no. 3, pp. 243–259, 2019. [CrossRef]
29. S. H. Li, X. H. Luo, and L. Z. Wu, "An improved whale optimization algorithm for locating critical slip surface of slopes," *Adv. Eng. Softw.*, vol. 157–158, p. 103009, 2021. [CrossRef]
30. D. Kumar, V. P. Singh, and M. A. Mallick, "Frequency control of interlinked microgrid system using fractional order controller," *Electrica*, vol. 24, no. 2, pp. 532–541, 2024. [CrossRef]

Dharmesh Kumar received his M. Tech degree from SLITE Longwal, Punjab, in 2008. Presently he is pursuing a Ph.D. degree from Integral University, Lucknow, in Electrical Engineering Department. His area of research is microgrid and renewable energy resources.

Vijay Pratap Singh (Senior Member, IEEE) received his PhD degree from the Motilal Nehru National Institute of Technology (MNNIT), Allahabad, India, in 2017. Presently, he is working as Senior Assistant Professor and Head of Electrical Engineering Department in Rajkiya Engineering College Sonbhadra. Dr. Singh received the prestigious best Teacher award from university in year 2020. His research area includes robust control applications in load frequency control and power quality in distributed generations and renewable energy resources, electric vehicles, smart grids, etc. He has many publications in national and international journals and conferences. He also served as reviewer of reputed national and international journals. He has served as a Reviewer for the IEEE "Transactions on Smart Grid, IEEE Transactions on Cybernetics, IEEE Transactions on Energy Conversion, IEEE Transaction on Industrial Applications, and IEEE Access." He has an interdisciplinary back ground and experience emphasizing on networked control systems and cyber-physical. systems for microgrid.

MA Mallick is professor in the Department of Electrical Engineering at Integral University Lucknow. His area of research is microgrid and renewable energy resources.