Detection and Defense Method Against False Data Injection Attacks for Distributed Load Frequency Control System in Microgrid

Zhixun Zhang, Jianqiang Hu, Jianquan Lu, Jie Yu, Jinde Cao, and Ardak Kashkynbayev

***Abstract*—In the realm of microgrid (MG), the distributed load frequency control (LFC) system has proven to be highly susceptible to the negative effects of false data injection attacks (FDIAs). Considering the significant responsibility of the distributed LFC system for maintaining frequency stability within the MG, this paper proposes a detection and defense method against unobservable FDIAs in the distributed LFC system. Firstly, the method integrates a bi-directional long short-term memory (BiLSTM) neural network and an improved whale optimization algorithm (IWOA) into the LFC controller to detect and counteract FDIAs. Secondly, to enable the BiLSTM neural network to proficiently detect multiple types of FDIAs with utmost precision, the model employs a historical MG dataset comprising the frequency and power variances. Finally, the IWOA is utilized to optimize the proportional-integral-derivative (PID) controller parameters to counteract the negative impacts of FDIAs. The proposed detection and defense method is validated by building the distributed LFC system in Simulink.**

***Index Terms*—Microgrid, load frequency control, false data injection attack, bi-directional long short-term memory (BiLSTM) neural network, improved whale optimization algorithm (IWOA), detection and defense.**

I. Introduction

THE microgrid (MG) is a significant component of the smart grid, which is an effective means to promote the utilization of renewable energy and alleviate the energy crisis. The traditional way of electricity production relies on fossil energy such as oil and coal, but these non-renewable energy sources will eventually be exhausted, and their pollutants will also seriously affect the natural environment, so it is a general trend to develop renewable energy such as wind and solar energy [1]-[4]. Since renewable energy is widely distributed, it is difficult to assure the stability of the MG when various distributed energy sources operate simultaneously, and the MG technology has been steadily developed to address this issue. The MG is autonomous, self-controlling, self-protecting, and self-managing small-scale power generation and distribution system that relies on renewable energy sources. It can operate in parallel with or independently from the external smart grid, thereby enhancing power system reliability and facilitating the growing integration of renewable energy [5].

The distributed load frequency control (LFC) system plays a crucial role in maintaining frequency stability in the MG. Imbalances between the power generation and load can cause significant fluctuations in system frequency, potentially resulting in unstable operation or equipment breakdown of the power system. The distributed LFC system effectively monitors the balance between load and power generation, ensuring frequency stability in the MG, especially in situations where power generations from various renewable energy sources are unstable [6], [7]. The LFC controller receives the area control error (ACE) from sensors and uses it to calculate control commands. These commands are then sent to generation units. The generation units adjust their output power according to the control commands, ensuring that power generation can follow load changes and thereby maintain frequency deviation within the allowed range of nominal value error. In addition, the urgency of frequency regulation requires that measurement devices in the distributed LFC system use simple encryption or no encryption, which unfortunately makes the distributed LFC system more vulnerable to various cyber attacks. These attacks could potentially cause the LFC controller to receive malicious instructions, resulting in significant fluctuations and deviations in system frequency, and severely compromising the stability of the MG. Therefore, it is crucial to ensure the security of the distributed LFC system to maintain the stability and reliable operation of the MG [8], [9].

With the continuous development of cyber-attack tech-

Manuscript received: June 10, 2023; revised: August 5, 2023; accepted: September 18, 2023. Date of CrossCheck: September 18, 2023. Date of online publication: November 13, 2023.

This work was supported in part by the National Natural Science Foundation of China (No. 61973078), in part by the Natural Science Foundation of Jiangsu Province of China (No. BK20231416), and in part by the Zhishan Youth Scholar Program from Southeast University (No. 2242022R40042).

Z. Zhang is with the School of Cyber Science and Engineering, Southeast University, Nanjing 210096, China (e-mail: zxzhangmw@seu.edu.cn).

J. Hu (corresponding author), J. Lu, and J. Cao are with the School of Mathematics, Southeast University, Nanjing 211189, China, J. Lu is also with the School of Electronic Information and Electrical Engineering, Chengdu University, Chengdu 610106, China, and J. Cao is also with the Yonsei Frontier Laboratory, Yonsei University, Seoul 03722, South Korea (e-mail: jqhu@seu. edu. cn; jqluma@seu.edu.cn; jdcao@seu.edu.cn).

J. Yu is with School of Electrical Engineering, Southeast University, Nanjing 210096, China (e-mail: yujie@seu.edu.cn).

A. Kashkynbayev is with the Department of Mathematics, Nazarbayev University, Nur-Sultan 010000, Kazakhstan (e-mail: ardak. kashkynbayev@nu. edu. kz).

DOI: 10.35833/MPCE.2023.000400

niques, the distributed LFC system is facing an increasing number of cyber-attacks. One of the most prevalent forms of these cyber-attacks is the false data injection attack (FDIA), in which the attacker cunningly constructs the attack vector to evade detection by the bad data detection (BDD) system in the MG [10]. The distributed LFC system, which combines cyberspace information technology with physical infrastructure, faces a real-time disadvantage that renders it susceptible to FDIAs during the communication process. These FDIAs can target the link between the sensor and the controller, causing the controller to receive data with false vectors. Subsequently, the controller may generate incorrect control instructions based on this manipulated data, thereby hindering the maintenance of frequency stability. Without implementing effective detection and defense mechanisms, FDIAs have the potential to severely compromise the overall stability of the MG. Consequently, it is imperative to implement appropriate measures to detect and defend against FDIAs within the MG, safeguarding the integrity and reliability of the distributed LFC system and the overall MG.

Since [11] proposes that attackers could employ FDIAs to evade detection by estimation residual-based BDD methods, there has been a substantial body of research works dedicated to the development of FDIAs. Several researchers have successfully demonstrated FDIAs with limited network information [12], [13]. Furthermore, [14] utilizes the self-attention generative adversarial network (SA-GAN) technique to create an effective FDIA that only requires exploiting easily accessible data. In the context of MG, [15] explores an FDIA capable of damaging generator synchronization systems.

As for the detection and defense mechanism of FDIAs on the power system, there exists two main types of methods: model-based detection and defense methods [16] - [21], and data-driven detection and defense methods [22]-[28]. Model-based detection and defense methods are dependent on predefined models that accurately depict the expected behavior of a system or network. These models are constructed using prior knowledge of the system attributes and anticipated conduct. Such models can take the form of rule-based, statistical, or deterministic approaches. Model-based detection and defense methods against FDIAs include cumulative sun [16], matrix separation [17], cooperative mechanism [18], [19], and observer-based methods [20], [21]. However, the adaptability and accuracy of model-based detection and defense methods can be restricted in handling novel threats and complex environments due to their dependence on prior knowledge and predefined models. Conversely, data-driven methods operate independently of predetermined models. They directly acquire insights into patterns and behaviors from the data without any presumptions about the normal behavior of the system. Employing machine learning and data mining techniques, these methods unearth concealed patterns and trends hidden within extensive datasets, and thus have better performance. The main data-driven technologies include deep learning [22], [23], and neural network [24]-[28].

Moreover, due to the importance of the LFC system, many researchers have studied the detection and defense of FDIAs in the LFC system in recent years. A method based on stochastic unknown input estimation (SUIE) has been proposed to estimate the state of LFC system for detecting FDIAs [29]. In [30], a defense mechanism that combines order observer and artificial neural network (ANN) has been proposed to resist FDIAs. Reference [31] suggests an observer-based control strategy for resisting FDIAs. Reference [32] proposes a method that combines fuzzy logic and neural network to detect multiple FDIAs. Reference [33] develops an LFC method based on a dynamic output feedback controller. Reference [34] considers a distributed event-triggered LFC algorithm based on bandwidth allocation to preserve the MG stability and maximize network resource utilization. Reference [35] proposes a method based on robust adaptive observer (RAO) to estimate existing FDIAs in the LFC system. By testing in various operational scenarios, a resilience-based MG frequency regulation mechanism has been presented to prevent network attacks and uncertainty of system characteristics [36]. Finally, real-time detection of FDIAs in LFC system is achieved by using sliding mode observer technology, and the position of the attacked system is located [37].

The existing detection and defense methods have certain limitations, which can be summarized in the following three categories.

1) Some researchers have considered few types of FDIAs and only proposed detection measures without subsequent defense measures. The generality of detection and defense measures across different types of FDIAs should be considered.

2) Model-based detection and defense methods rely heavily on the parameters of MGs. For example, SUIE [29] and RAO [35] strategies require accurate estimation of the system state, which may not always be possible or practical in real-world scenarios.

3) Some of the proposed defense methods such as bandwidth allocation and event-triggered algorithms [34] may introduce additional overhead and complexity to the system. Therefore, further research is needed to explore the effectiveness of current detection and defense methods in the face of multiple FDIAs.

Considering the limitations of previous detection and defense methods, this paper proposes a detection method that utilizes a bi-directional long short-term memory (BiLSTM) neural network and a defense method based on improved whale optimization algorithm (IWOA) to effectively combat FDIAs in distributed LFC systems in MG. To begin with, FDIAs can manifest in three distinct forms: pulse, step, and random. Subsequently, the BiLSTM neural network is trained offline using historical data from the MG, allowing for efficient utilization of system resources. Once trained, the network is integrated into the distributed LFC controller of the MG. Lastly, the IWOA optimizes the proportional-integral-derivative (PID) controller parameters in the distributed LFC system, ensuring stability even in the presence of FDIAs. The main contributions of this paper are described as follows.

1) A novel LFC model, which incorporates FDIA detec-

tion and defense, has been designed to effectively detect three types of FDIAs, including step, pulse, and random, and eliminate their negative impacts.

2) Given the temporal dependencies within the LFC system, where the current state is influenced not only by past but also by future states, a detection method utilizing the BiLSTM neural network has been introduced. This method adeptly captures information from past and future sequences, facilitating the precise detection of three types of FDIA.

3) Utilizing the IWOA, a defense method has been devised, which optimizes the parameters of the PID controller in the distributed LFC system after BiLSTM detects FDIA. This optimization enables the PID controller to maintain frequency deviation within the normal range, ensuring the stability of the MG even in the presence of FDIAs.

The remainder of this paper is organized as follows. The distributed LFC system in the MG is depicted in Section II. Section III discusses the proposed detection and defense method. The simulation results and analysis are presented in Section IV. Finally, Section V concludes this paper.

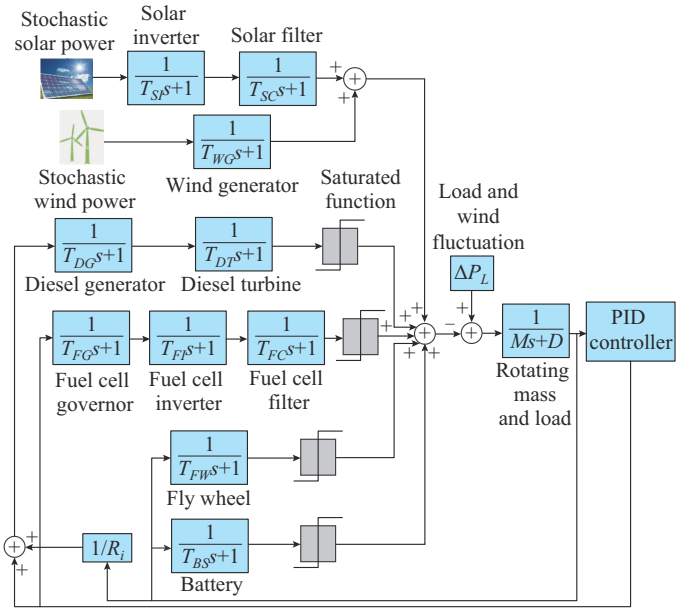

Fig. 1. Distributed LFC system of islanded MG.

II. Distributed LFC System in MG

The most essential feature of MG is its high level of autonomy, which allows for the localization and unitization of power supply and demand via autonomous coordination and control. At the same time, the high penetration of renewable energy in MG is a significant feature. Distributed wind and solar power technologies can efficiently conserve traditional fossil resources, reduce power generation expenses, and minimize pollutant emissions. The distributed LFC system of the islanded MG is considered in this section, as shown in Fig. 1. Energy storage technologies such as batteries and flywheels are included in the MG as well as renewable energies such as wind and solar power, other energy sources like diesel and gasoline, and variable loads. In Fig. 1, T_{SI}, T_{SC}, T_{WG}, T_{DG}, T_{DT}, T_{FG}, T_{FI}, T_{FC}, T_{FW}, and T_{BS} are the time constants of the solar inverter, solar filter, wind generator, diesel generator, diesel turbine, fuel cell governor, fuel cell inverter, fuel cell filter, fly wheel, and battery, respectively; R_i is the adjustment coefficient; ΔP_L is the load and wind fluctuation; M is the time constant of the rotating mass and load; and D is a damping coefficient.

A. Distributed LFC System Model

The function of the distributed LFC system is to maintain the frequency stability of the MG, ensuring its proper operation. Sensors in the distributed LFC system collect the system frequency deviation Δf and send it to the PID controller. The PID controller then generates the adjustment signal to modify the frequency based on Δf. The adjustment of PID controller ΔP_C can be represented as:

$$\Delta P_C = K_{Pi}\Delta f + K_{Ii}\int \Delta f + K_{Di}\Delta \dot{f} \tag{1}$$

where K_{Pi} is the proportional gains of the i^{th} power area; K_{Ii} is the integral gain of the i^{th} power area; and K_{Di} is the derivative gain of the i^{th} power area.

The state space equations of the LFC system in the MG can be expressed as:

$$\begin{cases} \dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}\boldsymbol{P}(t) + \boldsymbol{C}\boldsymbol{d}(t) \\ \boldsymbol{y}(t) = \boldsymbol{D}\boldsymbol{x}(t) \end{cases} \tag{2a}$$

where $\boldsymbol{x}(t)$ is the state variable vector, and $\boldsymbol{x}(t)=[\Delta f, \Delta P_{SC}, \Delta P_{SI}, \Delta P_{WG}, \Delta P_{DT}, \Delta P_{DG}, \Delta P_{FC}, \Delta P_{FI}, \Delta P_{FG}, \Delta P_{FW}, \Delta P_{BS}]^{\mathrm{T}}$, ΔP_{SC}, ΔP_{SI}, ΔP_{WG}, ΔP_{DT}, ΔP_{DG}, ΔP_{FC}, ΔP_{FI}, ΔP_{FG}, ΔP_{FW}, ΔP_{BS} are the solar filter, solar invert, wind generator, diesel turbine, diesel generator, fuel cell filter, fuel cell invert, fuel cell governor, fly wheel, and battery output power changes, respectively; $\boldsymbol{P}(t)$ is the input vector; $\boldsymbol{d}(t)$ is the load disturbance vector; $\boldsymbol{y}(t)$ is the output vector; $\boldsymbol{A}$ is the state matrix, and $\boldsymbol{A}_{21}=\boldsymbol{0}_{5\times 6}$; and $\boldsymbol{B}$, $\boldsymbol{C}$, and $\boldsymbol{D}$ are the input, load disturbance, and output matrices, respectively. These matrices are given as follows.

$$\boldsymbol{A} = \begin{bmatrix} \boldsymbol{A}_{11} & \boldsymbol{A}_{12} \\ \boldsymbol{A}_{21} & \boldsymbol{A}_{22} \end{bmatrix} \tag{2b}$$

$$\boldsymbol{A}_{11} = \begin{bmatrix} -\frac{D}{M} & -\frac{1}{M} & 0 & -\frac{1}{M} & -\frac{1}{M} & 0 \\ 0 & -\frac{1}{T_{SC}} & \frac{1}{T_{SC}} & 0 & 0 & 0 \\ 0 & 0 & -\frac{1}{T_{SI}} & 0 & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{T_{WG}} & 0 & 0 \\ 0 & 0 & 0 & 0 & -\frac{1}{T_{DT}} & \frac{1}{T_{DT}} \\ -\frac{1}{R_i T_{DG}} & 0 & 0 & 0 & 0 & -\frac{1}{T_{DG}} \end{bmatrix} \tag{2c}$$

$$\boldsymbol{A}_{12}=\begin{bmatrix} -\frac{1}{M} & 0 & 0 & -\frac{1}{M} & -\frac{1}{M} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{2d}$$

$$\boldsymbol{A}_{22}=\begin{bmatrix} -\frac{1}{T_{FC}} & \frac{1}{T_{FC}} & 0 & 0 & 0 \\ 0 & -\frac{1}{T_{FI}} & \frac{1}{T_{FI}} & 0 & 0 \\ 0 & 0 & -\frac{1}{T_{FG}} & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{T_{FW}} & 0 \\ 0 & 0 & 0 & 0 & -\frac{1}{T_{BS}} \end{bmatrix} \tag{2e}$$

$$\boldsymbol{B}=\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & \frac{1}{T_{DG}} & 0 & 0 & \frac{1}{T_{FG}} & 0 & 0 \end{bmatrix}^{\mathrm{T}} \tag{2f}$$

$$\boldsymbol{C}=\begin{bmatrix} -\frac{1}{M} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{T_{WG}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{\mathrm{T}} \tag{2g}$$

$$\boldsymbol{D}=\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{\mathrm{T}} \tag{2h}$$

B. FDIAs on Distributed LFC System

The LFC controller regulates the MG based on data coming from the frequency deviation line, and the security of the data is critical for the control commands of the LFC system. As shown in Fig. 2, the attack vector can be injected into the frequency deviation channel and remains hidden from the LFC controller, making it indistinguishable from the initial system state vector.

The residual test is used by the BDD system in the distributed LFC system to detect FDIAs, which can be expressed as:

$$\begin{cases} \boldsymbol{z}_a=\boldsymbol{z}+\boldsymbol{a} \\ \boldsymbol{x}_a=\boldsymbol{x}+\boldsymbol{c} \\ \left\| \boldsymbol{z}_a-\boldsymbol{H}\boldsymbol{x}_a \right\|_2=\left\| (\boldsymbol{z}-\boldsymbol{H}\boldsymbol{x})+(\boldsymbol{a}-\boldsymbol{H}\boldsymbol{c}) \right\|_2 \le \left\| \boldsymbol{z}-\boldsymbol{H}\boldsymbol{x} \right\|_2+ \\ \quad \left\| \boldsymbol{a}-\boldsymbol{H}\boldsymbol{c} \right\|_2 \le \boldsymbol{\alpha} \end{cases} \tag{3}$$

where $\boldsymbol{z}_a$ is the state variable with FDIAs; $\boldsymbol{a}$ is an injected attack vector; $\boldsymbol{z}$ is the state variable; $\boldsymbol{c}$ is the deviation of normal system states $\boldsymbol{x}_a$; $\boldsymbol{\alpha}$ is the threshold set by BDD system in advance; and $\boldsymbol{H}$ is the Jacobian matrix of the power system.

From the above equation, if the attack vector $\boldsymbol{a}$ satisfies the conditions in (4), this FDIA can successfully inject false data into the LFC system and not be detected by the residual test of the BDD system. In this paper, the FDIAs constructed all satisfy the conditions in (4). Three types of FDIAs including pulse, step, and random attacks are considered and described as follows.

$$\begin{cases} \boldsymbol{a}=\boldsymbol{H}\boldsymbol{c} \\ \left\| \boldsymbol{a}-\boldsymbol{H}\boldsymbol{c} \right\|_2 \le \boldsymbol{\alpha}-\left\| \boldsymbol{z}-\boldsymbol{H}\boldsymbol{x} \right\|_2 \end{cases} \tag{4}$$

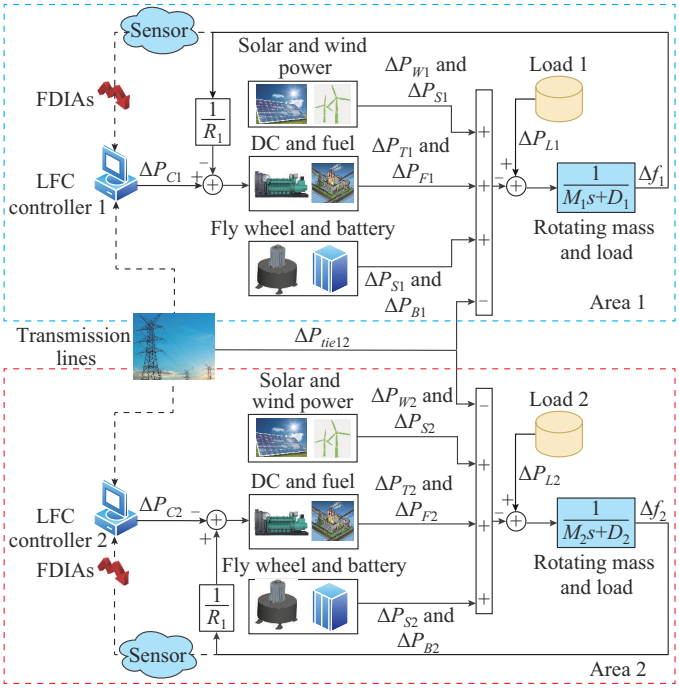

Fig. 2. Two-area interconnected MG system.

1) Pulse attacks (denoted by A_1): the attacker injects false data Δf_{a1} in the form of pulses over a period of time, which can be expressed as:

$$f_a(t)=\begin{cases} \Delta f_{a1} & t\in[t_{ia},t_{fa}] \\ 0 & \text{otherwise} \end{cases} \tag{5}$$

where $f_a(t)$ is the attack; t_{ia} is the initial time of the attack; and t_{fa} is the final time of the attack.

2) Step attacks (denoted by A_2): starting at a specific time, the attacker continuously injects false data Δf_{a2} into the LFC system, which can be expressed as:

$$f_a(t)=\begin{cases} 0 & t<t_{ia} \\ \Delta f_{a2} & t\ge t_{ia} \end{cases} \tag{6}$$

3) Random attacks (denoted by A_3): at random times, the attacker injects a false data Δf_{a3}, like sinusoidal, random, etc., which can be expressed as:

$$f_a(t)=\Delta f_{a3} \tag{7}$$

III. Proposed Detection and Defense Method

The proposed detection and defense method is demonstrated in this section. The BiLSTM neural network can detect three types of FDIAs proposed in this paper, and the IWOA can optimize the PID controller parameters to maintain the frequency deviation within the normal range.

A. BiLSTM Neural Network for Detection

The long short-term memory (LSTM) neural network is

an advanced form of recurrent neural network (RNN). Unlike traditional RNNs, the LSTM neural network addresses the issue of vanishing gradients that occur when there are too many layers. In such cases, the model gradually loses information over time, and during backpropagation, the error diminishes due to the vanishing gradient problem. As a result, the model struggles to effectively update the weights associated with previous time. This challenge is known as the "long-term dependency problem", which hampers the ability of the model to effectively capture information from past instances [38], [39].

To tackle this issue, researchers have both domestically and internationally made modifications to RNN models, and the LSTM neural network has emerged as the most prominent solution. The LSTM neural network maintains the chain structure of a traditional RNN but introduces a distinct repeating module structure with four layers. This design allows the LSTM neural network to retain valuable information while disregarding the less relevant parts to a certain extent, enabling long-term memory and enhancing the effectiveness of the model. The basic structure of LSTM neural network is illustrated in Fig. 3, where x_t is the input at time t; h_t is the hidden layer state at time t; h_{t-1} is the hidden layer state at time $t-1$; c_t is the internal state of the unit at time t; c_{t-1} is the internal state of the unit at time $t-1$; f_t is the forget gate; i_t is the input gate; $\tilde{c}_t$ is the input state at time t; o_t is the output gate; and σ is the sigmoid activation function.

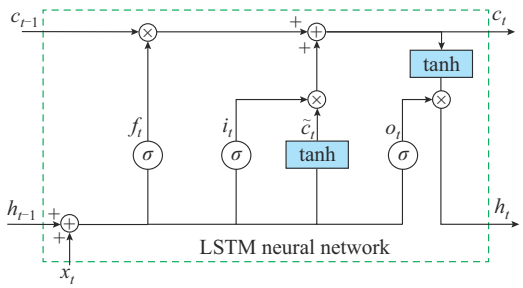

Fig. 3. Basic structure of LSTM neural network.

The LSTM neural network such as the RNN utilizes the internal state transfer to investigate the sequence element dependencies. To overcome the issue of gradient vanishing in RNNs, the LSTM neural network incorporates a gating mechanism. The gating link of LSTM is divided into three parts: forget, input, and output, with a state unit inserted to regulate the network operation.

1) Forget gate: the forget gate plays a crucial role in determining the extent to which the incoming information from the previous time step is retained at the current time. In (8), the forget gate f_t is computed by subjecting the linear transformation of the input x_t at time t and the hidden layer output h_{t-1} at time $t-1$ to an activation function σ. This ensures that the relevant information is retained while irrelevant information is discarded.

$$f_t=\sigma(\boldsymbol{W}_f[h_{t-1},x_t]+\boldsymbol{b}_f) \tag{8}$$

where $\boldsymbol{W}_f$ and $\boldsymbol{b}_f$ are the forget gate weight matrix and bias term matrix, respectively.

2) Input gate: the operation of the input gate primarily impacts the extent to which input information is retained at time t. The input gate i_t is shown in (9), and it is calculated similarly to the forget gate f_t.

$$i_t=\sigma(\boldsymbol{W}_i[h_{t-1},x_t]+\boldsymbol{b}_i) \tag{9}$$

where $\boldsymbol{W}_i$ and $\boldsymbol{b}_i$ are the input gate weight matrix and bias term matrix, respectively. $\tilde{c}_t$ is equivalent to integrating the state information contained in the input x_t, hidden layer h_{t-1} to form a new state quantity, and is shown in (10).

$$\tilde{c}_t=\tanh(\boldsymbol{W}_c[h_{t-1},x_t]+\boldsymbol{b}_c) \tag{10}$$

where $\boldsymbol{W}_c$ and $\boldsymbol{b}_c$ are the input state weight matrix and bias term matrix, respectively.

3) State unit: the main role of the state unit is to update the internal state of the LSTM neural network, transitioning the internal state c_t from the previous time to the current time. The state unit c_t at time t is shown in (11).

$$c_t=c_{t-1}f_t+\tilde{c}_t i_t \tag{11}$$

4) Output gate: the output gate controls the output at time t depending on the extent of c_t. The output gate o_t is shown in (12).

$$o_t=\sigma(\boldsymbol{W}_o[h_{t-1},x_t]+\boldsymbol{b}_o) \tag{12}$$

where $\boldsymbol{W}_o$ and $\boldsymbol{b}_o$ are the output gate weight matrix and bias term matrix, respectively. The hidden layer state output h_t is determined by both the internal state c_t together with the output gate o_t at time t, which is calculated as:

$$h_t=o_t\tanh(c_t) \tag{13}$$

Building upon the LSTM neural network, the BiLSTM neural network has been introduced. The BiLSTM neural network incorporates both the past and future states of the hidden layers, enabling for bidirectional and feedback connections between neural networks. This characteristic proves to be highly effective in identifying hidden relationships within time series data [40]. Considering that the state of the MG at the current time is influenced not only by the preceding state but also by the subsequent state, the BiLSTM neural network performs better in detecting FDIAs within the MG.

Figure 4 depicts the basic structure of BiLSTM neural network, which is a two-way cyclic structure with forward and backward propagation, and hidden layers for the past and future are independent of one another. The model output is y.

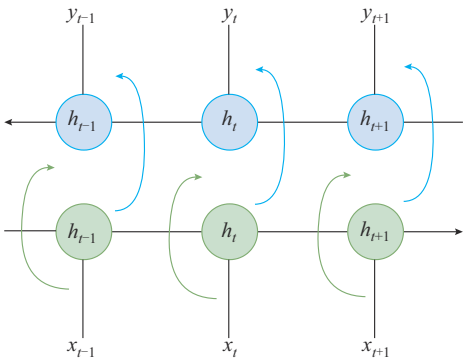

Fig. 4. Basic structure of BiLSTM neural network.

$$\begin{cases} \overleftarrow{h}_t = L(x_t, \overleftarrow{h}_{t-1}) \\ \overrightarrow{h}_t = L(x_t, \overrightarrow{h}_{t-1}) \end{cases} \tag{14}$$

where $\overleftarrow{h}_t$ is the hidden layer state of the forward LSTM neural network at time t; $\overrightarrow{h}_t$ is the hidden layer state of the reverse LSTM neural network at time t; and L is the LSTM cell. The overall hidden layer state of the network h_t is formed by combining $\overleftarrow{h}_t$ and $\overrightarrow{h}_t$. Figure 5 illustrates the detection procedure of the BiLSTM neural network. In this paper, three types of FDIAs are constructed, resulting in four labels for the BiLSTM neural network, as indicated in Table I. The defender first collects and preprocesses historical data from the MG to create a training set. The preprocessed data are then used to train the BiLSTM model, while the test set is utilized to validate the accuracy of the trained BiLSTM model. Ultimately, the trained model is employed to counteract FDIAs within the distributed LFC system of the MG.

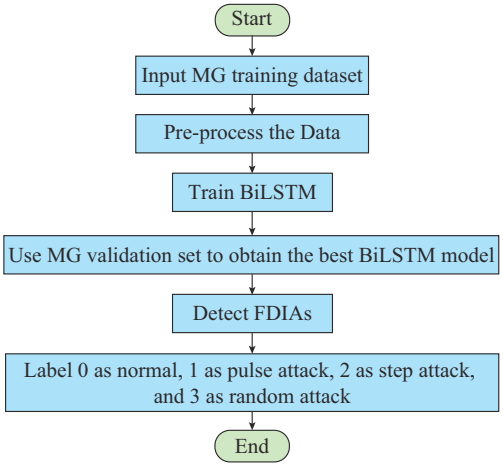

Fig. 5. Detection procedure of BiLSTM nerual network.

TABLE I
LABELS OF BILSTM NEURAL NETWORK

Label	Status
0	Normal
1	Pulse attacks
2	Step attacks
3	Random attacks

B. IWOA for Defense

The whale optimization algorithm (WOA) is a novel intelligent optimization method inspired by the predation behavior of whales. It offers advantages such as requiring fewer parameters, faster convergence, and improved accuracy. In WOA, each whale location represents a target solution, and the algorithm updates the positions using three methods: encircling prey, spiral search, and random search, to identify the optimal solution [41], [42]. To strike a balance between global and local search abilities, an improved version called the IWOA is proposed. The IWOA introduces a nonlinear convergence factor, which enhances its ability to handle large-scale complex optimization problems in the MG. By adjusting the convergence factor nonlinearly with the number of evolutionary selections and applying a diversity variation operation on the current optimal whale individuals, the IWOA effectively coordinates local and global search capabilities, reducing the risk of converging to a local optimum [43], [44].

To address the instability of the LFC system under FDIAs, the IWOA is proposed in this paper to defend against FDIAs. Upon receiving signals from the BiLSTM detection model, IWOA promptly optimizes the PID controller parameters in the LFC system. Leveraging its powerful global and local search capabilities, IWOA can find the optimal PID parameters, enabling the controller to effectively counteract the impact of FDIA and enhance the robustness and security of the LFC system. The optimization process of IWOA is illustrated as follows.

The position of the i^{th} individual in the d-dimensional space is represented by equation $\boldsymbol{X}_i = (X_i^1, X_i^2, \ldots, X_i^n)$, $i = 1, 2, \ldots, N$. Assuming that the number of whales engaging in predation is N and the space for searching for food is d-dimensional, the optimal solution corresponds to the position of the target prey.

1) The target prey is the current optimal solution in the optimization-seeking problem in IWOA, because the location of the target prey is unknown, and the whale accomplishes local optimization by surrounding the prey and spinning to update the location. Assuming that the location of the optimal whale in the current population is the individual closest to the value of the objective function, the location information of the global optimal solution is used to update the optimal whale's location by surrounding all other whale individuals in the population to the optimal whale location, and the whale surrounding prey behavior is given in (15). Assume that $p \in [0, 1]$ is the uniformly distributed random number. When $p < 0.5$ and $|A| < 1$ are equivalent, the whale swims in the current direction.

$$\begin{cases} X(t+1) = X_{\text{best}}(t) - AD \\ D = \left| CX_{\text{best}}(t) - X(t) \right| \\ A = 2\alpha r_1 - \alpha \\ C = 2r_2 \\ \alpha = 2 - 2T/T_{\max} \end{cases} \tag{15}$$

where T is the number of iterative searches; $T_{\max}$ is the maximum number of iterations; $X(t)$ is the whale position; $X_{\text{best}}(t)$ is the global optimal position; A and C are the coefficients; $r_1, r_2 \in [0, 1]$ are the uniformly distributed random numbers; and α is the convergence factor which can control the probability of the whale random searches and surround its prey.

2) When approaching the prey, the whale moves in a spiral, searching for the optimum of the many possible optimal solutions in the path, and the position is updated as in (16). When $p \geq 0.5$, the whale moves in the current direction.

$$X(t+1) = X_{\text{best}}(t) + D\mathrm{e}^{bl} \cos 2\pi l \tag{16}$$

where b is the constant that adjusts the spiral's shape; and l is a uniformly distributed random number located in the interval $[-1, 1]$.

3) When $|A| \geq 1$, the whale performs a random search out-

side the contraction envelope to discover the greatest state. The method randomly selects one whale from the current whale population as the global optimum solution, and the other whales in the population converge towards it. By updating the population's location in this way, the population's diversity and the global search capabilities of the algorithm are strengthened. The mathematical model is formulated as:

$$X(t+1)=X_{\text{rand}}(t)-A\left|CX_{\text{rand}}(t)-X(t)\right| \tag{17}$$

where X_{rand} is a random whale position.

The exploration ability of IWOA is mostly determined by the convergence factor α. When α is great, IWOA has a strong global search capability, while when α is small, IWOA has a stronger local search capability. As a result, in order to balance the relationship between the global and local searches, this paper introduces a nonlinear convergence factor enhancement method, as demonstrated in (18).

$$\alpha=\alpha_i-\alpha_f+\frac{1-I/T_{\max}}{1-\mu I/T_{\max}} \tag{18}$$

where α_i is the initial value of α; α_f is the final value of α; I is the current number of iterations; and μ is the linear weight. The defense method based on IWOA is summarized in Algorithm 1.

Algorithm 1: IWOA

Input: population size N, the maximum number of iteration $T_{\max}$, and dimension D
Initialize the whales population X_i ($i=1,2,\ldots,N$)
Calculate the fitness value of each individual and record the optimal PID parameters $X_{\text{best}}(t)=\{K_{Pt},K_{It},K_{Dt}\}$
while ($t<T$)
  for X_i ($i=1,2,\ldots,N$) **do**
  According to (15) and (18)
  Calculate α, A, and C
  Generate a random number p from 0 to 1
    if ($p<0.5$)
      if ($|A|<1$)
        Update the position of the search whale by (15)
      elseif ($|A|\geq 1$)
        Update the position of the search whale by (17)
      end if
      else if ($p\geq 0.5$)
        Update the position of the search whale by (16)
    end if
  end for
  Calculate the fitness of each whale
  Update the optimal PID parameters $X_{\text{best}}(t)$
end while
Output: optimal PID parameters $X_{\text{best}}(t)$

Remark 1: in this paper, according to the parameters and size of the MG, we set $\alpha_i=3$, $\alpha_f=1$, and $\mu=25$. The convergence factor α increases with the number of iterations at a smaller value in the early stage, and then decreases rapidly to a smaller value when the number of iterations increases. The improved convergence factor update strategy enables IWOA to have a strong global search capability in the early stage of the search, and ensures a faster convergence speed in the late stage of the search and prevents the algorithm from falling into local optimum.

C. MG with Detection and Defense Mechanism

In this paper, we leverage the sophisticated technologies of BiLSTM neural networks and IWOA to detect and mitigate FDIAs in MG. The method involves implementing a BiLSTM neural network and IWOA in a decentralized LFC system to scrutinize and forestall FDIAs in the prevailing distributed LFC data. By adopting this technique, we sustain the frequency deviation of MG within an acceptable range of error, thereby upholding its integrity and fortification.

The LFC system with detection and defence mechanism is illustrated in Fig. 6. It is integrated into the LFC controller framework, where trained BiLSTM neural networks scrutinize input data to identify grounds for suspicion. Upon detecting any probability of FDIAs, the IWOA receives an immediate signal and optimizes the PID controller parameters to counteract the frequency deviation engendered by FDIAs. As illustrated in Fig. 7, the detection and mitigation mechanism progresses in a systematic and disciplined manner. In case of the primary MG sustaining FDIAs, the LFC controller responds relative to frequency deviation data; such a response is typically subject to a time-lag and may not provide sufficient protection for the MG's security. The proposed method overcomes such shortcomings by delivering a comprehensive suite of detection and fortification mechanisms that effectively address the security issues facing MGs. Through promptly detecting FDIAs and optimizing PID controller parameters, the BiLSTM and IWOA deliver exceptional detection precision and defense capabilities. This bolsters the stability of the MG while ultimately preventing FDIAs. Moreover, the detection and defense mechanism proposed in this paper is specifically activated when FDIAs are present, and has no impact on the normal operation of the MG. It can be seamlessly integrated into the existing LFC controllers without the need for additional protection strategies, showcasing excellent scalability and requiring minimal investment.

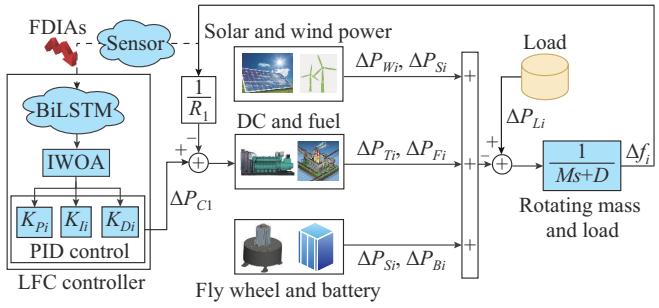

Fig. 6. LFC system with detection and defence mechanism.

IV. Simulation Results and Analysis

A. Parameters of MG and Three Types of FDIAs

This subsection identifies that the proposed detection and defense method is effective against FDIAs in the MG. The MG simulation model is illustrated in Fig. 1, and simulations have been performed in MATLAB/Simulink. The parameters of two-area interconnected MG are listed in Table II.

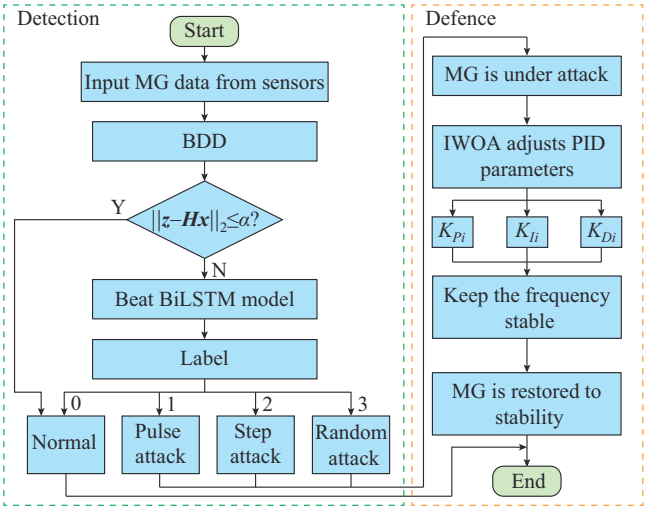

Fig. 7. Flow chart of detection and defence mechanism.

TABLE II
PARAMETERS OF TWO-AREA INTERCONNECTED MG

Parameter	Value
Rated load	$P_L = 1000$ MW
System frequency	$f = 50$ Hz
Adjustment coefficient	$R_i = 3$ Hz/p.u.
Solar inverter time constant	$T_{SI} = 0.04$ s
Solar filter time constant	$T_{SC} = 0.04$ s
Wind time constant	$T_{WG} = 1.5$ s
DEG governor time constant	$T_{DG} = 0.4$ s
DEG turbine time constant	$T_{DT} = 0.08$ s
Fuel cell governor time constant	$T_{FG} = 0.26$ s
Fuel cell inverter time constant	$T_{FI} = 0.04$ s
Fuel cell filter time constant	$T_{FC} = 0.004$ s
Fly wheel time constant	$T_{FW} = 0.1$ s
Battery time constant	$T_{BS} = 0.1$ s
Time constant	$M = 0.1667$ s
Damping coefficient	$D = 0.0015$ p.u./Hz

We have conducted simulations within 50 s to observe variations in wind power generation, solar power generation, and load perturbation. The random nature of wind power generation is demonstrated in Fig. 8. Compared with wind power, solar power has a comparatively stable pattern: the first 10 s exhibit an upward tendency, the next 40 s show a stable trend, and the stable power is 0.5 p.u.. Figure 9 depicts the schematic of solar power generation and the load perturbation curve. The load demand increases to 0.9 p.u. in the first 10 s, then gradually reduces to 0.5 p.u. between 10 and 40 s. Finally, the load maintains at 0.5 p.u. between 40 and 50 s.

In this paper, we design three different types of FDIAs to test the effectiveness of detection and defense method. The target of the FDIAs is the frequency measurement line.

1) Pulse attack: the first FDIA on the LFC system starts from $t = 10$ s with an attack $\Delta FDIA_1 = 0.8$ p.u..

2) Step attack: the second FDIA on the LFC system starts at $t = 10$ s with an attack $\Delta FDIA_2 = 0.2$ p.u..

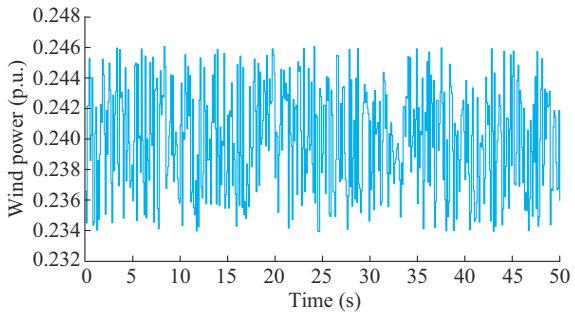

Fig. 8. Wind power generation of MG.

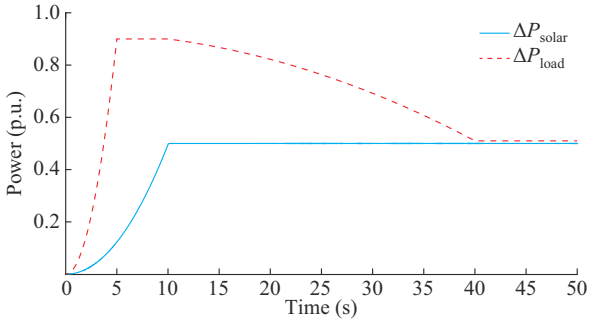

Fig. 9. Solar power generation and load perturbation curve of MG.

3) Random attack: the third FDIA consists of random form and sinusoidal form. The random FDIA starts at $t = 0$, and the attack $\Delta FDIA_3$ in the range of 0.095-0.115 p.u. is injected into the LFC system. The sinusoidal FDIA starts from $t = 0$, and the attack $\Delta FDIA_4$ in the range of 0.15-0.15 p.u. is injected into the LFC system.

B. Results and Analysis of Detection and Defence Method

The BiLSTM neural network is trained utilizing 39514 pieces of historical data from the MG, including 9596 pieces of normal data, 9528 pieces with the first FDIA, 9283 pieces with the second FDIA, and 9507 pieces with the third FDIA. The data are divided into a training set and a validation set, with the training set accounting for 70% of the total data set and the validation set accounting for 30%. The parameters of BiLSTM neural network are shown in Table III. The model consists of 100 hidden units and is trained for 250 epochs, with 1404 iterations per training epoch and a maximum iteration count of 351000. The training time for BiLSTM neural network is 108 min. As BiLSTM neural network is trained offline, it does not occupy the computational resources of the system. The learning rate is set to be 0.005 for the first 125 training epochs and then multiplied by a decay factor of 0.2 after 125 training epochs to reduce the learning rate and bring the model closer to the optimal solution. Secondly, the training accuracy and loss of the BiLSTM neural network after 250 training epochs are shown in Fig. 10. The graph demonstrates that these 250 training epochs perform excellently, with training accuracy approaching 90% and training loss remaining below 0.5.

Finally, the detection performance of the trained BiLSTM neural network is evaluated using the test set. Table IV compares our proposed model with other machine learning models based on accuracy, precision, recall, and F_1-score.

Among these models, the BiLSTM detection model proposed in this paper achieves the highest score in all four metrics, with an accuracy of 0.972 and an F_1-score of 0.911. This indicates that the BiLSTM model is superior in terms of its ability to detect FDIAs. Compared with other benchmark models such as SVM, LSTM, LSTM-attention, convolutional neural network long short-term memory (CNN-LSTM), gate recurrent unit (GRU), and bidirectional recurrent neural (BiGRU) network, the BiLSTM model outperforms them all by a significant margin, with the second-best F_1-score being 0.8817. These results demonstrate the effectiveness of the BiLSTM and its exceptional detection capability when applied to FDIAs.

TABLE III
PARAMETERS OF BILSTM NEURAL NETWORK

Parameter	Value
Input size	1
Number of classes	4
Number of hidden units	100
The maximum epochs	250
Gradient threshold	1
Initial learning rate	0.005
Learning rate drop period	125
Learning rate drop factor	0.2

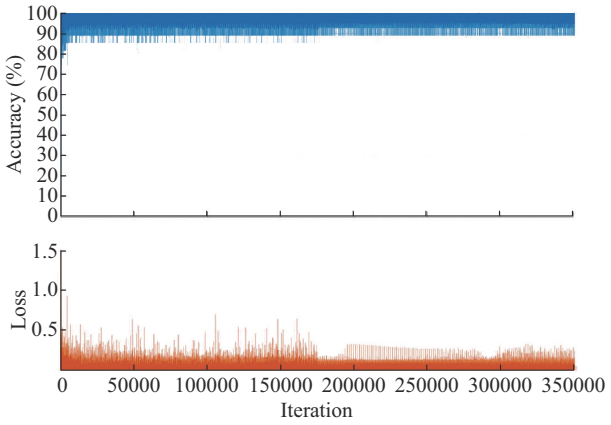

Fig. 10. Training accuracy and loss of BiLSTM neural network.

TABLE IV
DETECTION PERFORMANCE OF DEEP LEARNING MODELS FOR FDIAS

Model	Accuracy	Precision	Recall	F_1-score
SVM	0.7830	0.7558	0.6933	0.7234
LSTM	0.9035	0.8793	0.8264	0.8385
LSTM-attention	0.9254	0.8637	0.8396	0.8524
CNN-LSTM	0.9462	0.8812	0.8351	0.8575
GRU	0.9587	0.8973	0.8385	0.8669
BiGRU	0.9611	0.9063	0.8587	0.8817
BiLSTM	0.9720	0.9414	0.8829	0.9110

C. Results and Analysis of Defense Mechanism

This subsection describes the process of the defense research for the three types of FDIAs. As shown in Fig. 9, the load increases during the first 5 s, influencing the frequency deviation. The three different types of FDIAs are illustrated in Figs. 11-13. The original PID controller, as depicted in Figs. 14-17, does not correct the frequency deviation as the load develops, unlike the PID controller optimized by IWOA. The frequency deviation under the original PID controller adjustment can be as high as 0.05 p.u. or higher, but the frequency deviation under the PID controller optimized by IWOA adjustment is well within the usual error range and can be ignored. Moreover, to validate the performance of the IWOA, the WOA and particle swarm optimization (PSO) models are used for comparison. As shown in Figs. 14-17, the PID parameters optimized by WOA and PSO have resulted in oscillations that exceed the allowable error range when coping with the three different types of FDIAs, thus failing to maintain the stability of frequency. In contrast, IWOA eliminates the frequency fluctuations caused by FDIAs and maintains the stability of frequency within the normal error allowance range. Overall, these results demonstrate the superiority of IWOA over other optimization algorithms in mitigating the negative impacts of FDIAs on frequency stability.

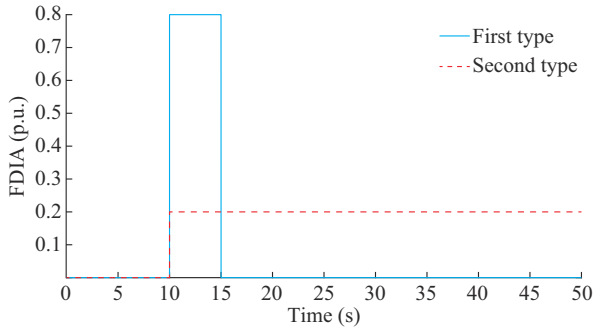

Fig. 11. First type and second type of FDIA.

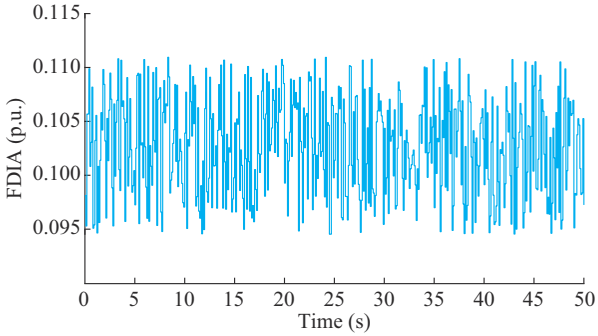

Fig. 12. Third type of FDIA (random FDIA).

The attacker employs an FDIA in pulse type and injects false data into the MG at $t = 10$ s. The MG controlled by the PID controller has a large frequency deviation at $t = 10$ s, almost close to –0.1 p.u., and the MG is in an unstable state for the next 40 s. To mitigate the instability caused by the FDIA, the MG by IWOA rapidly starts to adjust after being subjected to FDIA at $t = 10$ s, bringing the frequency deviation back to zero in a short time, and the MG remains in a stable state for the next 40 s, as shown in Fig. 14. The PID controller optimized by IWOA successfully resists the FDIA in pulse type.

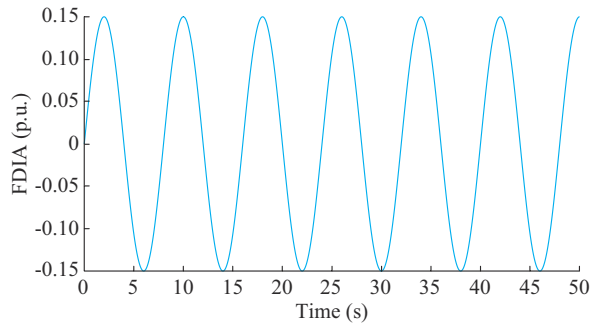

Fig. 13. The third type of FDIA (sinusoidal FDIA).

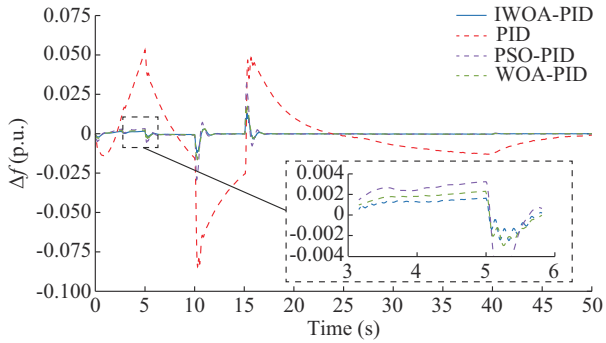

Fig. 14. Δf in the first type of FDIA controlled by original PID controller and PID controller optimized by IWOA.

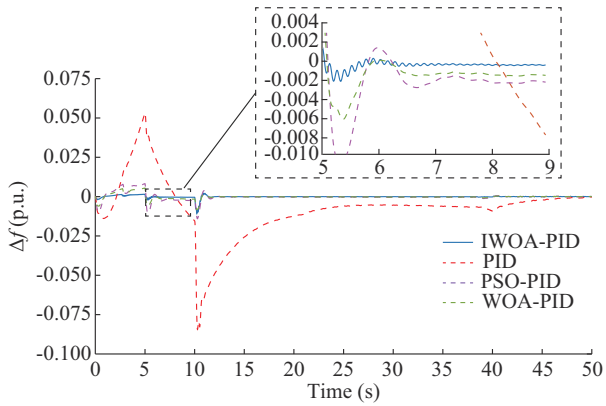

Fig. 15. Δf in the second type of FDIA controlled by original PID controller and PID controller optimized by IWOA.

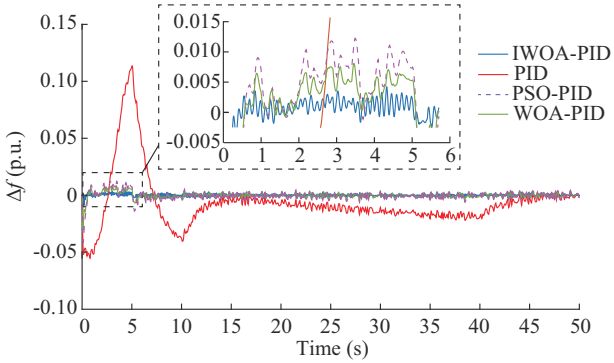

Fig. 16. Δf in random FDIA controlled by original PID controller and PID controller optimized by IWOA.

In the second type of FDIA, the attacker continuously injects false data into the system at $t=10$ s, as shown in Fig. 11. The MG operated by the PID controller exhibits a large frequency oscillation during the first 5 s, as illustrated in Fig. 15, and the stability of the MG is severely disrupted. At $t=10$ s, the stability of the MG is threatened once more because the attacker injects false data, causing the frequency deviation to reach −0.1 p.u.. The BiLSTM neural network detects the presence of the FDIA in the MG and sends a defense signal to IWOA, then the PID controller optimized by IWOA controlled MG quickly implements defensive measures and calculates the optimal PID controller parameters at this time and maintains the frequency deviation within the error tolerance throughout, demonstrating that the proposed PID controller optimized by IWOA can still preserve the MG stable under the FDIA in step type.

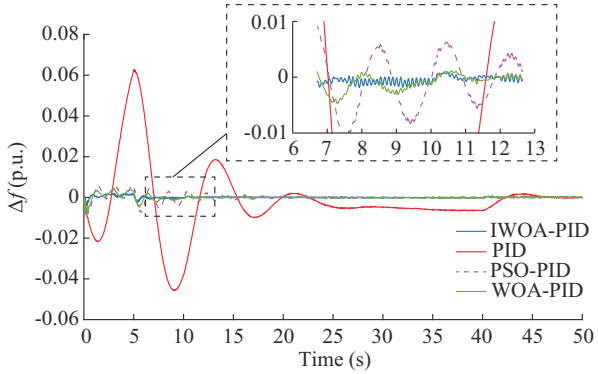

Fig. 17. Δf in sinusoidal FDIA controlled by original PID controller and PID controller optimized by IWOA.

In the third type of FDIA, the attacker employs a random FDIA with the attack vector including random and sine signals, as shown in Figs. 12 and 13, to attack the LFC system. The frequency deviation is shown in Fig. 16. The random FDIAs have a greater impact on the system than the two types of FDIA mentioned earlier. The LFC system controlled by the PID controller cannot cope with this type of FDIA, and the frequency deviation always remains in a large oscillation state. Under the random signal, the frequency deviation is up to 0.12 p.u. and down to −0.05 p.u., while under the sine signal, the frequency deviation is up to 0.06 p.u. and down to −0.05 p.u.. The frequency oscillates for 50 s, posing a significant threat to the stability of the MG. On the other hand, the IWOA-based defense mechanism proposed in this paper can react promptly after receiving the defense signal from BiLSTM. Even when reacting to the random FDIAs, its adjusted frequency deviation is completely within the allowable error range, ensuring the frequency stability of the MG.

Given the inherent stochastic nature of metaheuristic techniques such as PSO and WOA, in their search strategies, this paper compares different intelligent optimization algorithms using statistical data. Fifty experiments have been conducted to optimize the PID controller using PSO, WOA, and IWOA, respectively. The algorithms are executed multi-

ple times using different random seeds, with the seed values randomly selected between 50 and 30 to mitigate the influence of random type of FDIA. Finally, Fig. 18 presents the absolute frequency deviation $|\Delta f|$ of different intelligent optimization algorithms under three different types of FDIAs. It can be observed that IWOA performs the best among the three FDIAs, as it keeps the frequency deviation within a stable range, effectively maintaining the frequency stability. This also validates the effectiveness of using IWOA to defend against FDIAs in this paper.

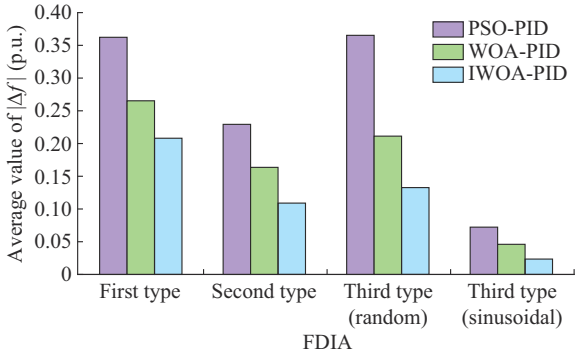

Fig. 18. $|\Delta f|$ of different optimization algorithms under different types of FDIAs.

In summary, the attacker can use different ways of FDIA to damage the MG. The detection method based on the BiLSTM neural network can detect three forms of FDIAs presented in this paper promptly, with a detection accuracy of 0.9720. After receiving the defense signal from BiLSTM neural network, the IWOA-based defense mechanism presented in this paper immediately optimizes the PID controller to resist the negative impacts of multiple types of FDIAs. Figures 14-17 demonstrate the generalizability of this paper for defending against different FDIAs in MG.

V. Conclusion

This paper is devoted to designing detection and defensive techniques to handle with FDIAs in distributed LFC systems. Firstly, a detection and defense model is integrated into the LFC controller to detect and eliminate the negative impact of FDIAs. Furthermore, the BiLSTM neural network trained offline performs the detection, and simulation results confirm its accuracy. Finally, the defense method utilizes IWOA to optimize the PID controller parameters to maintain the system frequency deviation within the rated range, ensuring the stability of the MG even when affected by FDIAs. Simulation results demonstrate the effectiveness of the proposed detection and defense method in mitigating various types of FDIAs and maintaining MG stability. Future work will focus on defensive techniques to combat adversarial machine learning in MGs.

References

[1] B. Zhou, J. Yang, C. Y. Chung *et al.*, "Multi-microgrid energy management systems: architecture, communication, and scheduling strategies," *Journal of Modern Power Systems and Clean Energy*, vol. 9, no. 3, pp. 463-476, May 2021.

[2] T. Adefarati and R. C. Bansal, "Reliability, economic and environmental analysis of a microgrid system in the presence of renewable energy resources," *Applied Energy*, vol. 236, pp. 1089-1114, Feb. 2019.

[3] S. K. Tiwari, B. Singh, and P. K. Goel, "Design and control of microgrid fed by renewable energy generating sources," *IEEE Transactions on Industry Applications*, vol. 54, no. 3, pp. 2041-2050, May 2018.

[4] J. Hu, Z. Zhang, J. Lu *et al.*, "Demand response control of smart buildings integrated with security interconnection," *IEEE Transactions on Cloud Computing*, vol. 10, no. 1, pp. 43-55, Jan. 2022.

[5] J. Li, Y. Liu, and L. Wu, "Optimal operation for community-based multi-party microgrid in grid-connected and islanded modes," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 756-765, Mar. 2016.

[6] H. H. Alhelou, M.-E. Hamedani-Golshan, R. Zamani *et al.*, "Challenges and opportunities of load frequency control in conventional, modern and future smart power systems: a comprehensive review," *Energies*, vol. 11, no. 10, p. 2497, Sept. 2018.

[7] M.-H. Khooban, T. Niknam, M. Shasadeghi *et al.*, "Load frequency control in microgrids based on a stochastic noninteger controller," *IEEE Transactions on Sustainable Energy*, vol. 9, no. 2, pp. 853-861, Apr. 2017.

[8] D. Du, M. Zhu, X. Li *et al.*, "A review on cybersecurity analysis, attack detection, and attack defense methods in cyber-physical power systems," *Journal of Modern Power Systems and Clean Energy*, vol. 11, no. 3, pp. 727-743, May 2023.

[9] Q. Zhou, M. Shahidehpour, A. Alabdulwahab *et al.*, "A cyber-attack resilient distributed control strategy in islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 3690-3701, Sept. 2020.

[10] D. Liu, A. Dyśko, Q. Hong *et al.*, "Transient wavelet energy-based protection scheme for inverter-dominated microgrid," *IEEE Transactions on Smart Grid*, vol. 13, no. 4, pp. 2533-2546, Jul. 2022.

[11] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1-33, Jun. 2011.

[12] X. Liu, Z. Bao, D. Lu *et al.*, "Modeling of local false data injection attacks with reduced network information," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1686-1696, Jul. 2015.

[13] X. Liu and Z. Li, "Local topology attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 2617-2626, Nov. 2016.

[14] R. Jiao, G. Xun, X. Liu *et al.*, "A new AC false data injection attack method without network information," *IEEE Transactions on Smart Grid*, vol. 12, no. 6, pp. 5280-5289, Nov. 2021.

[15] A. S. Mohamed, M. F. M. Arani, A. A. Jahromi *et al.*, "False data injection attacks against synchronization systems in microgrids," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4471-4483, Sept. 2021.

[16] M. N. Kurt, Y. Yilmaz, and X. Wang, "Real-time detection of hybrid and stealthy cyber-attacks in smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 498-513, Feb. 2019.

[17] K. Huang, Z. Xiang, W. Deng *et al.*, "False data injection attacks detection in smart grid: a structural sparse matrix separation method," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 3, pp. 2545-2558, Sept. 2021.

[18] S. Sahoo, S. Mishra, J. C.-H. Peng *et al.*, "A stealth cyber-attack detection strategy for DC microgrids," *IEEE Transactions on Power Electronics*, vol. 34, no. 8, pp. 8162-8174, Aug. 2019.

[19] Y. Chen, D. Qi, H. Dong *et al.*, "A FDI attack-resilient distributed secondary control strategy for islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 1929-1938, May 2021.

[20] A. Cecilia, S. Sahoo, T. Dragičević *et al.*, "On addressing the security and stability issues due to false data injection attacks in DC microgrids: an adaptive observer approach," *IEEE Transactions on Power Electronics*, vol. 37, no. 3, pp. 2801-2814, Mar. 2021.

[21] M. Shi, X. Chen, M. Shahidehpour *et al.*, "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, May 2021.

[22] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505-2516, Sept. 2017.

[23] Y. Zhang, J. Wang, and B. Chen, "Detecting false data injection attacks in smart grids: a semi-supervised deep learning approach," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 623-634, Jan. 2021.

[24] C. Chen, Y. Chen, J. Zhao *et al.*, "Data-driven resilient automatic generation control against false data injection attacks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 12, pp. 8092-8101, Dec. 2021.

[25] S. D. Roy, S. Debbarma, and J. M. Guerrero, "Machine learning based multi-agent system for detecting and neutralizing unseen cyber-attacks in AGC and HVDC systems," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 12, no. 1, pp. 182-193, Mar. 2022.
[26] M. R. Habibi, H. R. Baghaee, T. Dragičević *et al.*, "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, Oct. 2021.
[27] M. R. Habibi, H. R. Baghaee, F. Blaabjerg *et al.*, "Secure MPC/ANN-based false data injection cyber-attack detection and mitigation in DC microgrids," *IEEE Systems Journal*, vol. 16, no. 1, pp. 1487-1498, Mar. 2022.
[28] Z. Zhang, J. Hu, J. Lu *et al.*, "Preventing false data injection attacks in LFC system via the attack-detection evolutionary game model and KF algorithm," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 6, pp. 4349-4362, Dec. 2022.
[29] A. Ameli, A. Hooshyar, A. H. Yazdavar *et al.*, "Attack detection for load frequency control systems using stochastic unknown input estimators," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2575-2590, Oct. 2018.
[30] A. Abbaspour, A. Sargolzaei, P. Forouzannezhad *et al.*, "Resilient control design for load frequency control system under false data injection attacks," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 9, pp. 7951-7962, Sept. 2020.
[31] M. R. Khalghani, J. Solanki, S. K. Solanki *et al.*, "Resilient frequency control design for microgrids under false data injection," *IEEE Transactions on Industrial Electronics*, vol. 68, no. 3, pp. 2151-2162, Mar. 2021.
[32] Z. Chen, J. Zhu, S. Li *et al.*, "Detection of false data injection attacks on load frequency control system with renewable energy based on fuzzy logic and neural networks," *Journal of Modern Power Systems and Clean Energy*, vol. 10, no. 6, pp. 1576-1587, Nov. 2022.
[33] H. Javanmardi, M. Dehghani, M. Mohammadi *et al.*, "BMI-based load frequency control in microgrids under false data injection attacks," *IEEE Systems Journal*, vol. 16, no. 1, pp. 1021-1031, Mar. 2021.
[34] M. M. Hossain, C. Peng, H.-T. Sun *et al.*, "Bandwidth allocation-based distributed event-triggered LFC for smart grids under hybrid attacks," *IEEE Transactions on Smart Grid*, vol. 13, no. 1, pp. 820-830, Jan. 2022.
[35] J. Ye and X. Yu, "Detection and estimation of false data injection attacks for load frequency control systems," *Journal of Modern Power Systems and Clean Energy*, vol. 10, no. 4, pp. 861-870, Jul. 2022.
[36] D. K. Mishra, P. K. Ray, L. Li *et al.*, "Resilient control based frequency regulation scheme of isolated microgrids considering cyber attack and parameter uncertainties," *Applied Energy*, vol. 306, p. 118054, Jan. 2022.
[37] A. D. Syrmakesis, H. H. Alhelou, and N. D. Hatziargyriou, "Novel SMO-based detection and isolation of false data injection attacks against frequency control systems," *IEEE Transactions on Power Systems*, doi: 10.1109/TPWRS.2023.3242015.
[38] B. Lindemann, B. Maschler, N. Sahlab *et al.*, "A survey on anomaly detection for technical systems using LSTM networks," *Computers in Industry*, vol. 131, p. 103498, Oct. 2021.
[39] M. Ma and Z. Mao, "Deep-convolution-based LSTM network for remaining useful life prediction," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 1658-1667, Mar. 2021.
[40] X. Zuo, C. Zhang, F. Cong *et al.*, "Driver distraction detection using bidirectional long short-term network based on multiscale entropy of EEG," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 10, pp. 19309-19322, Oct. 2022.
[41] X. Chen, L. Cheng, C. Liu *et al.*, "A WOA-based optimization approach for task scheduling in cloud computing systems," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3117-3128, Sept. 2020.
[42] D. Kong, Y. Chen, N. Li *et al.*, "Tool wear estimation in end milling of titanium alloy using NPE and a novel WOA-SVM model," *IEEE Transactions on Instrumentation and Measurement*, vol. 69, no. 7, pp. 5219-5232, Jul. 2019.
[43] S. M. Bozorgi and S. Yazdani, "IWOA: an improved whale optimization algorithm for optimization problems," *Journal of Computational Design and Engineering*, vol. 6, no. 3, pp. 243-259, Feb. 2019.
[44] S. Li, X. Luo, and L. Wu, "An improved whale optimization algorithm for locating critical slip surface of slopes," *Advances in Engineering Software*, vol. 157, p. 103009, Jul. 2021.

Zhixun Zhang received the B.S. degree in network engineering from North Minzu University, Yinchuan, China, in 2020. He is currently working toward the Ph.D. degree with the School of Cyber Science and Engineering, Southeast University, Nanjing, China. His research interests include security and protection of smart grid, and defense methods against false data injection attack.

Jianqiang Hu received the B.S. degree in mathematics and applied mathematics from the North China University of Water Resources and Electric Power, Zhengzhou, China, in 2010, the M.S. degree in applied mathematics from Southeast University, Nanjing, China, in 2013, and the Ph.D. degree in control theory and control engineering, Southeast University, in 2016. Currently, he is an Associate Professor with Jiangsu Provincial Key Laboratory of Networked Collective Intelligence and Department of System Science of School of Mathematics, Southeast University. His current research interests include distributed optimization and control of multiagent systems, and demand-side control in smart grids.

Jianquan Lu received the B.S. degree in mathematics from Zhejiang Normal University, Jinhua, China, in 2003, the M.S. degree in mathematics from Southeast University, Nanjing, China, in 2006, and the Ph.D. degree in applied mathematics from City University of Hong Kong, Hong Kong, China, in 2009. From 2010 to 2012, he was an Alexander von Humboldt Research Fellow in PIK, Potsdam, Germany. He is currently a Professor at the Department of Systems Science, School of Mathematics, Southeast University. His current research interests include collective behavior in complex dynamical networks and multi-agent systems, logical networks, and hybrid systems.

Jie Yu received the B.S., M.S., and Ph.D. degrees in electricial engineering from Southeast University, Nanjing, China, in 1996, 2000, and 2009, respectively. She was a Power System Monitoring Software Engineer with the State Grid Electric Power Research Institute, Nanjing, China, from 2000 to 2006. Currently, she is an Associate Professor with the School of Electrical Engineering, Southeast University. Her research interests include power optimal dispatch, renewable generation, and power system monitoring technology.

Jinde Cao received the B.S. degree in mathematics/applied mathematics from Anhui Normal University, Wuhu, China, in 1986, the M.S. degree in mathematics/applied mathematics from Yunnan University, Kunming, China, in 1989, and the Ph.D. degree in mathematics/applied mathematics from Sichuan University, Chengdu, China, in 1998. He was a Postdoctoral Research Fellow at the Department of Automation and Computer-aided Engineering, Chinese University of Hong Kong, Hong Kong, China, from 2001 to 2002. He is an Endowed Chair Professor, Dean of the School of Mathematics, and Director of the Research Center for Complex Systems and Network Sciences at Southeast University, Nanjing, China. He is also the Director of the National Center for Applied Mathematics at Southeast University, and Director of the Jiangsu Provincial Key Laboratory of Networked Collective Intelligence of China. He is elected as a Member of Russian Academy of Sciences, Member of the Academy of Europe, Member of Russian Academy of Engineering, Member of the European Academy of Sciences and Arts, Member of the Lithuanian Academy of Sciences, Fellow of African Academy of Sciences, and Fellow of Pakistan Academy of Sciences. His research interests include complex networks and complex systems, neural dynamics and optimization, and engineering stability.

Ardak Kashkynbayev received the Ph.D. degree from the Department of Mathematics, Middle East Technical University, Ankara, Turkey, in 2016. Currently, he is an Assistant Professor at the Department of Mathematics, Nazarbayev University, NurSultan, Kazakhstan. His research interests include difference and differential equations, mathematical biology, and neural networks.