Detection of False Data Injection Attacks on Load Frequency Control System with Renewable Energy Based on Fuzzy Logic and Neural Networks

Ziyu Chen, Jizhong Zhu, Shenglin Li, Yun Liu, and Tengyan Luo

***Abstract*—Load frequency control (LFC) system may be destroyed by false data injection attacks (FDIAs) and consequently the security of the power system will be impacted. High-efficiency FDIA detection can reduce the damage and power loss to the power system. This paper defines various typical and hybrid FDIAs, and the influence of several FDIAs with different characteristics on the multi-area LFC system is analyzed. To detect various attacks, we introduce an improved data-driven method, which consists of fuzzy logic and neural networks. Fuzzy logic has the features of high applicability, robustness, and agility, which can make full use of samples. Further, we construct the LFC system on MATLAB/Simulink platform, and systematically simulate the experiments that FDIAs affect the LFC system by tampering with measurement data. Among them, considering the large-scale penetration of renewable energy with intermittency and volatility, we generate three simulation scenarios with or without renewable energy generation. Then, the performance for detecting FDIAs of the improved method is verified by simulation data samples.**

***Index Terms*—Load frequency control (LFC), wind turbine and photovoltaic generation, fuzzy logic, neural network.**

I. Introduction

WITH the speedy development of computation, communication, and control technology [1], today's smart grid has developed into a cyber-physical system (CPS), which is deeply integrated by cyber and physical systems [2]. Load frequency control (LFC) system connects cyber and physical systems, which is an important part related to the communication network and executed by supervisory control and data acquisition (SCADA) [3]. The proportional-integral (PI) LFC program is widely used to adjust the frequency deviation and tie-line power of multi-area power system. In the LFC system, the power and frequency measurements of generators in each control area are transmitted to control center through the communication network [4]. Due to the close connection between LFC system and communication part, and the dependence of the smart grid on data communication in addition to physical failures, the modern power system is also threatened by cyber attacks.

Cyber attacks may seriously affect the secure and steady operation of the power system by destroying important information on critical infrastructures [5]. Relay protection performed in a predetermined manner may not be effective for CPS [6], because it is not determined whether the failure is caused by physical or cyber factors. False data injection attack (FDIA) is a relatively common cyber attack, and it is highly challenging [7]. FDIAs fight the LFC system and bypass the error data detection of SCADA, and then lead to the state estimation bias and the wrong decisions of SCADA [8], which makes the system unstable and affects power economic dispatch [9]. Many research works have been devoted to studying the possible means of constructing FDIAs. One of the generally recognized methods is that the attacker obtains part of the configuration information of the power system and can operate some variable measurement values [10]. For example, from March 2019 to April 2019, the power system of Venezuelan suffered FDIAs that caused widespread power outages. Experts speculated that the attackers corrupted the real information based on the configuration information and related parameters of the system, and maliciously destroyed the control performance [11]. Moreover, unlike other cyber attacks such as jamming and distributed denial of service, FDIAs can avoid the traditional detection mechanisms that are residual-based bad data [10]. Therefore, it is significant to analyse the influence of FDIAs on LFC system and recognize FDIAs efficiently. In this paper, we conduct the study on FDIAs, destroying the power system by tampering with measurement data.

In the past few years, research works on the impacts of FDIAs and the corresponding detection methods have received a lot of attention. In a wide range of FDIA detection solutions, two directions are mainly involved: model-based detection and data-driven detection. The former mainly contains estimation-based or residual-based methods. Reference [12] constructs different attack scenarios, and proposes the FDIAs whose principle is to track the dynamic changes of measurement errors based on Kullback-Leibler distance (KLD). After FDIAs are infiltrated into the power grid, the

Manuscript received: August 8, 2021; revised: November 14, 2021; accepted: January 25, 2022. Date of CrossCheck: January 25, 2022. Date of online publication: May 6, 2022.

This work was partly funded by the Science and Technology Planning Project of Guangdong Province of China (No. 2020A0505100004).

Z. Chen, J. Zhu (corresponding author), S. Li, Y. Liu, and T. Luo are with the School of Electric Power Engineering, South China University of Technology, Gunagzhou 510640, China (e-mail: epchenzy@mail.scut.edu.cn; zhujz@scut.edu.cn; iamlshl@126.com; lyscut@scut.edu.cn; epluoty@mail.scut.edu.cn).

DOI: 10.35833/MPCE.2021.000546

probability distributions of measurement deviations deviate from historical samples, which leads to a more serious KLD. Reference [13] presents a decentralized identification program according to the Markov graph of bus phase angle. It uses the conditional covariance threshold test to study the grid construction. The model-based methods are proposed by the experiments for detecting FDIAs by comparing the state estimation value with the real-time measurement value. Reference [14] evaluates the network security of static state estimation of power system with the possibility of phasor measurement units. Attacks are considered on the metric function of the Jacobian matrix or state estimation. However, the accuracy of these methods is highly related to the accuracy of the models and parameters of the power system [15]. The slight uncertainty in mathematical models and parameters may cause low detection performance.

As for data-driven detection method, it does not require a real physical model. Data-driven detection method relies on historical data to train statistical models, i.e., to find the relationship between the input features and the output variables, e.g., the types of FDIAs. However, a single method ordinarily has certain limitations. Specifically, the classic support vector machine (SVM) [16] only gives the two-class classification algorithm. In the usage of data mining, it is usually necessary to deal with the multi-class classification scenario. Pattern trees (PTs) [17] are relatively difficult to detect the patterns in the sequence. Long short-term memory (LSTM) networks [18] are a special kind of recurrent neural networks (NNs). LSTM networks have large computational complexity and need more computational cost. In addition, although LSTM networks can learn long-term dependencies, they still face the problem of vanishing and exploding gradients. When the time steps are relatively long, the information may not be transmitted to the later time steps. Moreover, overfitting may happen after the training of backpropagation NNs [19], which will affect the accuracy of detection. Faced with the above challenges, the paper proposes an improved method for detecting FDIAs, which is data-driven and composed of fuzzy logic and neural networks (FNNs). Fuzzy logic has the characteristics of high applicability, robustness, and agility, which can make full use of data [20]. NNs have the features of simple structure, strong generalization ability, and nonlinear mapping [21]. Reference [22] shows that FNNs can identify the faults in building automation systems and accurately classify the characteristics of various faults. Reference [23] indicates that FNNs can accurately detect and perform the islanding. Reference [24] expresses that in a liquid-level modeling of an industrial coke furnace, when input or output information is available, FNNs are very useful for nonlinear system recognition. However, there is no research work on the detection of FDIAs on LFC system with wind turbine (WT) or photovoltaic (PV) power generation based on FNNs. Due to the rapid development of renewable energy (RE) power generation, the intermittency and volatility of its output also affect the safety and stability of modern power system. The RE generation system is added to the simulation system, which makes the experiment more diverse and practical.

To detect the FDIAs accurately and quickly, this paper introduces an improved data-driven detection method, which is a combination of fuzzy logic and NNs, and has the characteristics of strong robustness, agility, and generalization ability. The performance of the method is verified by detecting various types of FDIAs on the dynamic simulation model of LFC with RE generation. The detailed contributions of this paper can be summarized as follows.

1) The model of multi-area LFC system with RE generation is set up. The two-area and four-area LFC systems are simulated based on MATLAB/Simulink platform in three scenarios, respectively. They are the LFC system without RE generation, the LFC system with RE generation in one area, and the LFC system with RE generation in each of the two areas.

2) The typical and hybrid FDIAs with various characteristics are defined, and the impacts of various FDIAs on two-area and four-area LFC systems in different simulation scenarios are simulated and analyzed.

3) An improved method is proposed, then the fault detection results through the improved method are compared with NNs, fuzzy pattern trees (FPTs), and LSTM, from which the performance of the improved method is proven.

The rest of this paper is organized as follows. Section II indicates the dynamic model of multi-area LFC system with RE generation. (Section III introduces an improved method for detecting FDIAs. Section IV defines the various typical and hybrid FDIAs.) In Section V, the impacts of different FDIAs on the two-area and four-area LFC systems are simulated based on MATLAB/Simulink platform, and the performance of the improved method for detecting FDIAs is evaluated. Section VI summarizes this paper and plans future works.

II. Dynamic Model of Multi-area LFC System

Figure 1 presents the dynamic model of the multi-area LFC system with RE generation. Each area of the simulation includes several basic components, among which are governor, turbine, generator, and PI controller. The PI controller is used to wipe out the area control error (ACE). In Fig. 1, a and b in the superscript and subscript denote the a^{th} and b^{th} areas, res pectively ΔP_{ab} is the tie-line power deviation flowing from the a^{th} area to the b^{th} area; R_a and R_b are the governor droop control factors of the a^{th} and b^{th} areas, respectively; K_P^a and K_I^a are the proportional and integral gains of the a^{th} area, respectively; T_g^a and T_{ch}^a are the time constants of governor and turbine of the a^{th} area, respectively; T_{ab} is the tie-line synchronizing co-efficiency between the a^{th} and b^{th} areas; ΔP_v^a, ΔP_m^a, and ΔP_d^a are the deviations of power output, generator mechanical output, and load of the a^{th} area, respectively; P_{WT}^a and P_{PV}^a are the outputs of WT and PV power generation systems of the a^{th} area, respectively; $P_{sys,base}$ is the base power of the multi-area LFC system; ΔP_{RE}^a is the output deviation of RE generation of the a^{th} area; M_a is the inertia moment of generator of the a^{th} area; D_a is the damping coefficient of unit of the a^{th} area; u_a is the signal of turbine control of the a^{th} area; and c_a and c_b are the transmission channels of FDIA measurement data of the a^{th} and b^{th}

areas, respectively.

In the multi-area LFC system, each generation unit in all the control areas can be simplified into an equivalent generation part. The ACE is defined as:

$$ACE_a = \beta_a \Delta f_a + \Delta P_{tie}^a \tag{1}$$

where ACE_a is the ACE of the a^{th} area, $a, b = 1, 2, \ldots, l$ are the indices of areas, and l is the number of areas in the multi-area LFC system; β_a is the frequency bias factor of the a^{th} area; Δf_a is the frequency deviation of the a^{th} area; and ΔP_{tie}^a is the tie-line exchange power deviation of the a^{th} area.

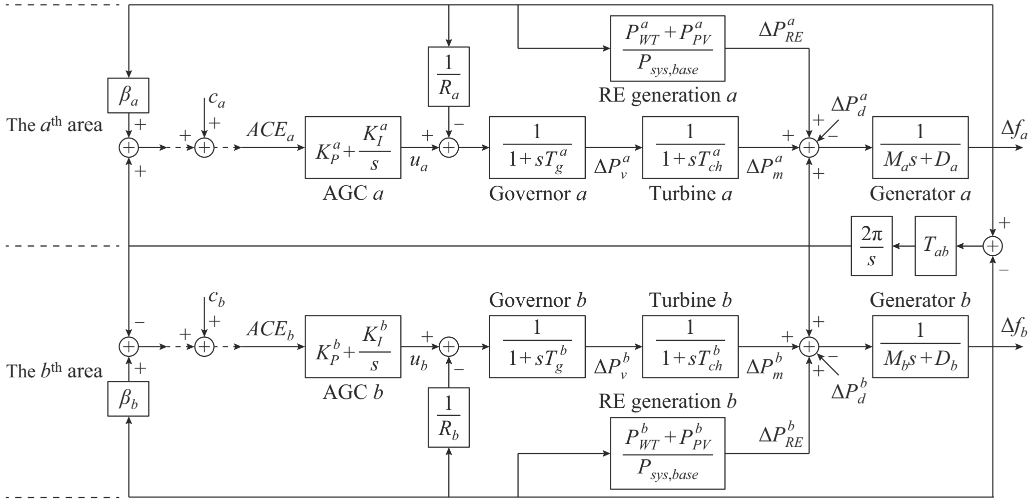


Fig. 1. Dynamic model of multi-area LFC system with RE generation.

As for the uncertainty and intermittence of WT/PV power generation system, when the RE generation system is added to the LFC system, there are not only power constraints, but also power balance constraints, which can maintain the relative stability of load and power generation.

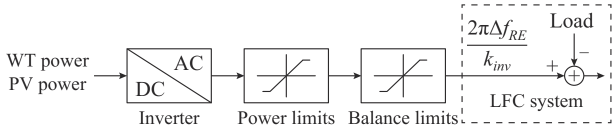


Fig. 2. Limits of RE generation system.

As illustrated in Figs. 1 and 2, the equations for dynamic model of the multi-area LFC system are:

$$\begin{cases} \dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}\boldsymbol{u}(t) + \boldsymbol{F}\left(\Delta \boldsymbol{P}_d^L - \dfrac{2\pi\Delta f_{RE}^a}{k_{inv}}\right) \\ \boldsymbol{y}(t) = \boldsymbol{C}\boldsymbol{x}(t) \end{cases} \tag{2}$$

where $\boldsymbol{x}$ is the state vector; $\boldsymbol{u}$ is the control vector; $\boldsymbol{y}$ is the output vector; $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$, $\boldsymbol{F}$, and $\Delta \boldsymbol{P}_d^L$ are the system matrices; k_{inv} is the droop factor; Δf_{RE}^a is the frequency deviation of the inverter in the a^{th} area of RE generation system; $\boldsymbol{x}(t) = \left[x_1(t)\ x_2(t)\ \ldots\ x_L(t)\right]^{\mathrm{T}}$; $\boldsymbol{x}_a(t) = \left[\Delta f_a\ \Delta P_m^a\ \Delta P_v^a\ \int ACE_a\ \Delta P_{tie}^a\right]$; $\boldsymbol{y}(t) = \left[y_1(t)\ y_2(t)\ \ldots\ y_L(t)\right]^{\mathrm{T}}$; $\boldsymbol{y}_a(t) = \left[ACE_a\ \int ACE_a\right]^{\mathrm{T}}$; $\boldsymbol{u}(t) = \left[u_1(t)\ u_2(t)\ \ldots\ u_L(t)\right]^{\mathrm{T}}$; $\boldsymbol{B} = \operatorname{diag}\left[B_1\ B_2\ \ldots\ B_L\right]$; $\boldsymbol{B}_a = \begin{bmatrix} 0 & 0 & \dfrac{1}{T_g^a} & 0 & 0 \end{bmatrix}$; $\boldsymbol{C} = \operatorname{diag}\left[C_1\ \ C_2\ \ \ldots\ \ C_L\right]$; $\boldsymbol{C}_a = \begin{bmatrix} \beta_a & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$; $\boldsymbol{F} = \operatorname{diag}\left[F_1\ \ F_2\ \ \ldots\ \ F_L\right]$; $\boldsymbol{F}_a = \begin{bmatrix} -\dfrac{1}{M_a} & 0 & 0 & 0 & 0 \end{bmatrix}$; $\boldsymbol{A} = \begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1L} \\ A_{21} & A_{22} & \cdots & A_{2L} \\ \vdots & \vdots & & \vdots \\ A_{L1} & A_{L2} & \cdots & A_{LL} \end{bmatrix}$; $\boldsymbol{A}_{ab} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -2\pi T_{ab} & 0 & 0 & 0 & 0 \end{bmatrix}$; $\Delta \boldsymbol{P}_d^L(t) = \left[\Delta P_d^1(t)\ \ \Delta P_d^2(t)\ \ \ldots\ \ \Delta P_d^L(t)\right]^{\mathrm{T}}$;

and $$\boldsymbol{A}_{aa} = \begin{bmatrix} -\dfrac{D_a}{M_a} & \dfrac{1}{M_a} & 0 & 0 & -\dfrac{1}{M_a} \\ 0 & -\dfrac{1}{T_{\mathrm{ch}}^a} & \dfrac{a}{T_{\mathrm{ch}}^a} & 0 & 0 \\ -\dfrac{1}{R_a T_g^a} & 0 & -\dfrac{1}{T_g^a} & 0 & 0 \\ \beta_a & 0 & 0 & 0 & 1 \\ 2\pi \displaystyle\sum_{b=1, b\neq a}^{L} T_{ab} & 0 & 0 & 0 & 0 \end{bmatrix}.$$

III. FNNs

In this section, an improved method for detecting FDIAs is proposed, which is based on data-driven method and composed of FNNs [20]. Fuzzy logic can make full use of data, which has the characteristics of high agility. The structure of NNs is simple, and it has the feature of strong generalization ability, and nonlinear mapping [21].

A. Fuzzy Aggregation

Fuzzy aggregation is a logical operator of fuzzy set or fuzzy membership value [25]. There are several categories, including triangular-conorm (T-conorm), triangular-norm (T-norm), and averaging operator. T-norm is proposed by Schweizer and Sklar, the averaging operator of which is divided into weighted averaging (WA) and ordered-WA (OWA) [26], [27]. As demonstrated in Table I, the fundamental T-norm and T-conorm pairs operate separately based on u and v ($u, v \in [0,1]$), which are fuzzy membership values.

TABLE I
FUNDAMENTAL T-NORM AND T-CONORM PAIRS

Name	T-norm	T-conorm
Min/max	$\min\{u,v\} = u \wedge v$	$\max\{u,v\} = u \vee v$
Algebraic	uv	$u+v-uv$
Lukasiewicz	$\max\{u+v-1, 0\}$	$\min\{u+v, 1\}$
Einstein	$\dfrac{uv}{2-(u+v-uv)}$	$\dfrac{u+v}{1+uv}$

The WA operator of dimension m is a map about $Q^m \to Q$, which has an related m-element vector $\boldsymbol{r}_i = [r_1 \quad r_2 \quad \dots \quad r_m]^{\mathrm{T}}$, $r_j \in [0, 1]$, $1 \le j \le m$, and $\sum_{j=1}^{m} r_j = 1$; then, the WA is defined as:

$$WA(u_1, u_2, \dots, u_m) = \sum_{i=1}^{m} r_i u_i \tag{3}$$

Similarly, the OWA is defined as:

$$OWA(u_1, u_2, \dots, u_m) = \sum_{i=1}^{m} r_i g_i (u_1, u_2, \dots, u_m) \tag{4}$$

where $g_i(u_1, u_2, \dots, u_m)$ returns the i^{th} largest element of the collection $(u_1, u_2, \dots, u_m)$. Among them, the prime differentiation between WA and OWA operators is that the OWA has no special weight w_j related to an element, while the weights are related to the specific ordered locations of the elements.

In short, it is straightforward to extend forenamed aggregation to fuzzy item: the consequence of the aggregation of two fuzzy items is a novel fuzzy item, and the aggregation is employed between the two fuzzy items in pairs.

B. Structure of FNN

FNN is the improved model based on fuzzy logic and NNs for detecting FDIAs in this paper. The frame of FNNs is shown in Fig. 3, which includes four layers.

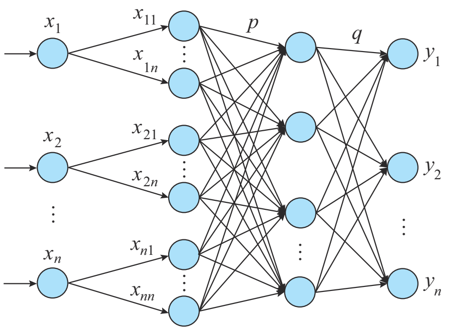


Fig. 3. Frame of FNNs.

In the first layer, the neuron nodes of input layer are used to input samples. The data sets generated by different FDIAs on the multi-area LFC system are the input samples of FNNs, which include 10 features such as the ACE value, deviation values of measurement frequency, real frequency, attack frequency, power output, and mechanical output and load of the generator. The second layer is fuzzy input layer. It is applied to produce new fuzzy items that can fully mirror the features of input data. Then, the third layer is hidden layer. The connection of these hidden layers has the most important feature of FNNs. The neuron nodes of fuzzy input layer and hidden layer are connected with each other. Specifically, the information is transmitted from input layer to fuzzy input layer, and then to hidden layer and output layer (the last layer). Final output results are compared with the sample values to calculate the accuracy [28]. The neuron nodes in adjacent layers are fully connected and expressed as weights, and the neuron nodes in the same layer are not connected with each other. The improved method contains two phases. One is the forward transmission of the signals, and the other is the backward transmission of the errors. As shown in Fig. 3, $x_i (i = 1, 2, \dots, n)$ are the input samples; $x_{il} (i, l = 1, 2, \dots, n)$ are the data samples processed by fuzzy method; p is the connection of neuron nodes of fuzzy input and hidden layer as weight; q is the connection of neuron nodes of hidden layer and output layer as weight; and $y_i (i = 1, 2, \dots, n)$ is the output results. The formula for the hidden layer $f^n(j)$ is:

$$f^n(j) = \sum_{il} p^n_{il,j} x_{il} \tag{5}$$

where $p^n_{il,j}$ is the connection of neuron nodes of fuzzy input and hidden layer as the weight in the n^{th} iteration, l indicates the number of fuzzy items obtained by fuzzy method, and i and il are the numbers of neuron nodes of input layer and those of fuzzy input layer, respectively. The formula of the output layer is:

$$\hat{y}^n(k) = \sum_{j} q^n_{j,k} f^n(j) \tag{6}$$

where $\hat{y}^n(k)$ is the output result after the n^{th} iteration; $q^n_{j,k}$ is the connection of neuron nodes of hidden layer and those of output layer as weight in the n^{th} iteration; and k is the number of neuron nodes of output layer.

In order to make the network outputs as close as possible to the actual results, output errors can be fed back in the direction from the output layer to input layer. The gradient correction method [29] is used to adjust the weights between the neuron nodes of each layer and the threshold θ of each neuron node. The structure of the FNNs is determined after meeting the accuracy requirements. The calculation output error in the n^{th} iteration e^n is:

$$e^n = \frac{1}{2} \sum_{k} (y(k) - \hat{y}^n(k))^2 \tag{7}$$

where $y(k)$ is the actual sample value. The equations of correction weights in the $(n+1)^{\text{th}}$ iteration are:

$$q^{n+1}_{j,k} = q^n_{j,k} + \Delta q^{n+1}_{j,k} \tag{8}$$

$$p^{n+1}_{il,j} = p^n_{il,j} + \Delta p^{n+1}_{il,j} \tag{9}$$

Let η denote the learning rate, we can obtain:

$$\Delta q_{j,k}^{n+1} = -\eta \frac{\partial e}{\partial q_{j,k}^{n}} \tag{10}$$

$$\Delta p_{il,j}^{n+1} = -\eta \frac{\partial e}{\partial p_{il,j}^{n}} \tag{11}$$

Besides, the improved method includes a training phase and a testing phase. The data samples from FDIAs in multi-area LFC system are separated into training groups and testing groups. During the training phase of FNNs, in the fuzzy input layer, the features of input variables can be better extracted in unsupervised learning. Then, in the supervised learning, the regularization method [30] is used to alleviate the overfitting of the training sets.

IV. Types of Attacks

As shown in the Fig. 1, c_a and c_b are the transmission channels of FDIA measurement data, and various attacks are added to the multi-area LFC system through the measurement channels. The control center accepts measurement values as input and processes them to obtain the output control signal. The attackers can manipulate measurement values so that any operational decisions based on these measurement values may trigger the control operations unwarranted for the real system state [31]. In this section, we define several types of attack templates as follows.

A. Typical Attack

1) Scaling Attack

Scaling attack can affect system rapidly and trigger the load shedding scheme. The scaling attack modifies measurement value by injecting scaling parameter to make it proportionally higher or lower than the actual value c_s. We define the system equations as:

$$Z_{mea,CA} = \begin{cases} Z_{rea} & \forall t \notin t_a \\ Z_{rea} + CA & \forall t \in t_a \end{cases} \tag{12}$$

$$CA = c_s Z_{rea} \tag{13}$$

where t is the running time of the dynamic system; CA is the scaling attack value; Z_{rea} is the real value; and $Z_{mea,CA}$ is the measurement value under scaling attack.

2) Ramp Attack

A ramp function changes with the time gradually at a constant rate. Ramp attack alters the measurement by adding $c_r t_a$, where c_r is the factor of ramp attack and t_a is the attack period. We can define the system of equations as:

$$Z_{mea,RA} = \begin{cases} Z_{rea} & \forall t \notin t_a \\ Z_{rea} + RA & \forall t \in t_a \end{cases} \tag{14}$$

$$RA = c_r t_a \tag{15}$$

where RA is the value of ramp attack; and $Z_{mea,RA}$ is the measurement value under ramp attack.

3) Sine Attack

Sine attack is a type of attack that changes the measurement value in cycles, causing it to oscillate continuously. During the attack, as the sine wave fluctuates, the measurements are periodically set to higher or lower values. We can define the system of equations as:

$$Z_{mea,SA} = \begin{cases} Z_{rea} & \forall t \notin t_a \\ Z_{rea} + SA & \forall t \in t_a \end{cases} \tag{16}$$

$$SA = \sin t_a \tag{17}$$

where SA is the sine attack value; and $Z_{mea,SA}$ is the measurement value under sine attack.

B. Hybrid Attack

Scaling-ramp attack (SRA) modifies the measurement value by simultaneously injecting the scaling and ramp attacks. Scaling-sine attack (SSA) tampers the measurement value by injecting the scaling and sine attacks at the same time. Ramp-sine attack (RSA) alters the measurement value by simultaneously infiltrating the ramp and sine attacks.

Typical and hybrid FDIAs are maliciously injected to the multi-area LFC system through c_a and c_b, which causes errors in the measurement values, leads the control center to make wrong decisions, and affects the safe and stable operations of CPS.

V. Simulation Studies and Analysis

The experiments are implemented on a desktop computer with i7-9700 CPU at 3.00 GHz, 16 GB of RAM, 64-bit Windows. The base power of experiment system is 100 MW and the experimental simulations are based on per-unit data. The parameters of the two-area LFC system are illustrated in Table II.

TABLE II
Parameters of Two-area LFC System

Parameter	Value (p.u.)	Parameter	Value (p.u.)
R	0.05	β	21
k_P, k_I	1, 0.3	T_{12}	0.1986
M	10	D	1
T_g	0.1	T_{ch}	0.3

The values of WT-PV power are obtained from the Elia Group. As shown in Fig. 4, the outputs of WT-PV power generation system are illustrated in detail.

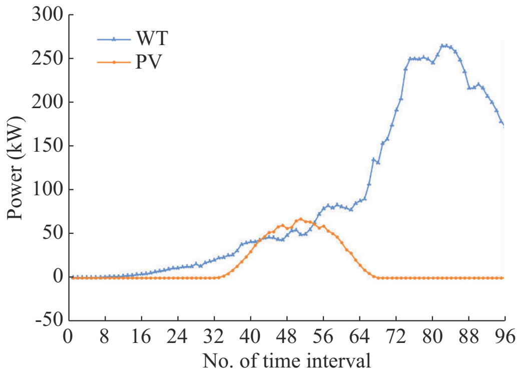


Fig. 4. Output of WT-PV power generation system.

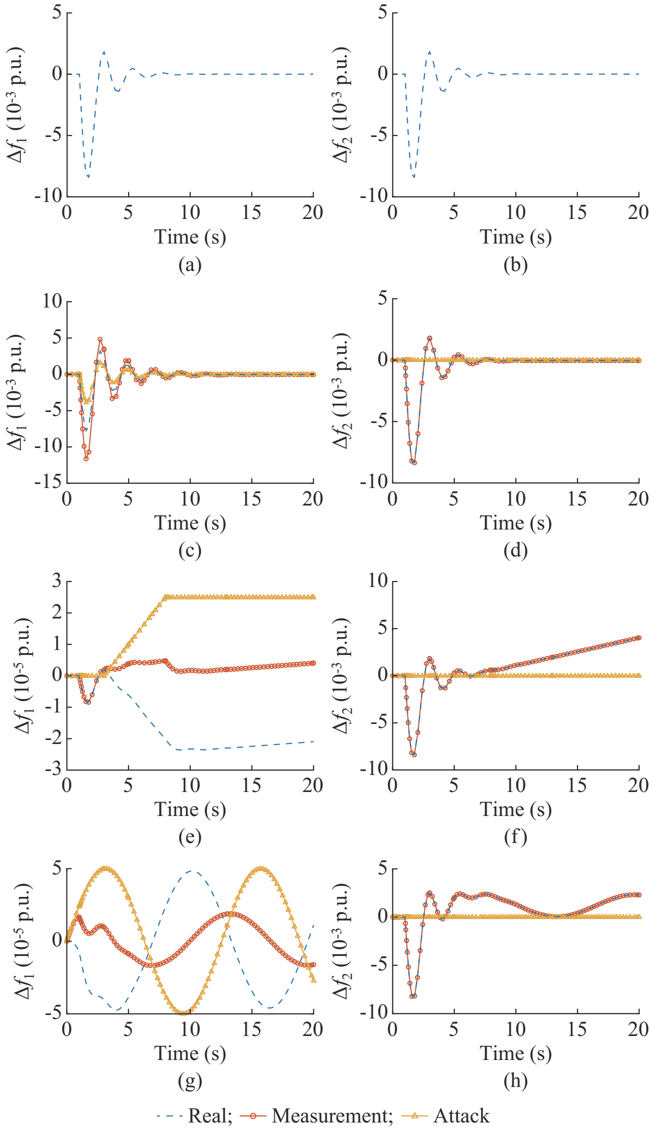
The value of WT power gradually increases over time, and reaches the maximum value at about the 80th time interval, because of high wind speed at night. The value of PV power attains the peak at the 50th time interval, due to the strong sunlight at noon.

A. Impacts of FDIAs on Two-area LFC System

In this subsection, the impacts of different typical FDIAs on the two-area LFC system will be analyzed. Area 1 and area 2 of the two-area LFC system are the same, and the simulation system is set up in three environments. The experiment is based on MATLAB/Simulink platform.

1) Frequency Deviations Without WT-PV Power Generation System

Figure 5 demonstrates the frequency deviations of the two-area LFC system without WT-PV power generation under different attacks on area 1. The real value reflects the actual state of system operation, and the measurement value is the superimposed result of the real and attack effects.



(a) (b) (c) (d) (e) (f) (g) (h)

Fig. 5. Frequency deviations of two-area LFC system without WT-PV power generation under different attacks on area 1. (a) Δf_1 under normal circumstances. (b) Δf_2 under normal circumstances. (c) Δf_1 under a scaling attack on area 1. (d) Δf_2 under a scaling attack on area 1. (e) Δf_1 under a ramp attack on area 1. (f) Δf_2 under a ramp attack on area 1. (g) Δf_1 under a sine attack on area 1. (h) Δf_2 under a sine attack on area 1.

FDIAs can cause errors in the measurement values, which may lead to mistakes in control decisions and affect normal operations. As indicated in Fig. 5(a) and (b), under the normal circumstance, the real frequency deviation values of two areas are interfered in the first second due to the sudden change of load, whose value is 0.2. And after a short oscillation, the values become steady. When the scaling attack with a scaling parameter of 0.5 is injected into area 1, as denoted in Fig. 5(c), the real frequency deviation amplitude of area 1 changes proportionally, and the duration of fluctuation increases. At the same time, comparing Fig. 5(b) and (d), the real frequency deviation value of area 2 has not changed. When a ramp attack is injected into area 1, it has a slope of 0.005 and an upper limit of 0.025, as shown in Fig. 5(e) and (f). In area 1, as the attack value increases, the real frequency deviation value decreases. When the attack value becomes fixed, the real frequency deviation of area 1 slowly increases. Due to the influence of area 1, the real frequency deviation of area 2 fluctuates for a while, then it keeps increasing and cannot reach the equilibrium. After a sine attack with the amplitude of 0.05 and the frequency of 0.5 is injected to area 1, the relevant results are demonstrated in Fig. 5(g) and (h). As the attack value fluctuates periodically in area 1, the real frequency deviation value of area 1 waves irregularly within a certain range, then it changes with the cycle. Due to the influence of area 1 and the mutation load with the value of 0.2 in the first second, the real frequency deviation value of area 2 fluctuates within a periodic after a period of shock.

2) Frequency Deviations with WT-PV Power Generation System in Area 1

Figure 6 shows the frequency deviations of the two-area LFC system with WT-PV power generation in area 1 under different attacks on area 1. Comparing Fig. 6(a) with Fig. 5(a), under normal circumstances, these two pictures are symmetric about the *x*-axis, which represents the WT-PV power generation system as the power generation module, and its output value is twice the load value. Likewise, Fig. 6(c) and Fig. 5(c) are also *x*-axis symmetric. Figure 6(e) and Fig. 5(e) are symmetrical about the *x*-axis in the first three seconds. Comparing Fig. 6(g) with Fig. 5(g), under a sine attack in area 1, the amplitude is 0.05 p.u. and the frequency is 0.5 p.u.. The real frequency deviation value has minor changes in the first three seconds; however, it still fluctuates with the the cycle afterwards. Comparing the Fig. 6(b), (d), (f), and (h) with Fig. 5(b), (d), (f), and (h), it can be observed that they are exactly the same, meaning that adding the WT-PV power generation system with appropriate capacity to area 1 has no effect on area 2.

Figure 7 reveals the frequency deviations of the two-area LFC system with WT-PV power generation in area 1 under different attacks on area 2. Comparing Fig. 7(b) with Fig. 5(b), it can be observed that when the scaling attack is injected into area 2, it has a scaling parameter of 0.5. The real frequency deviation value of area 2 fluctuates more strongly and the fluctuation lasts longer, but it eventually stabilizes. At the same time, comparing Fig. 7(a) with Fig. 6(a), it can be observed that the real frequency deviation value of area 1 has not changed at all.

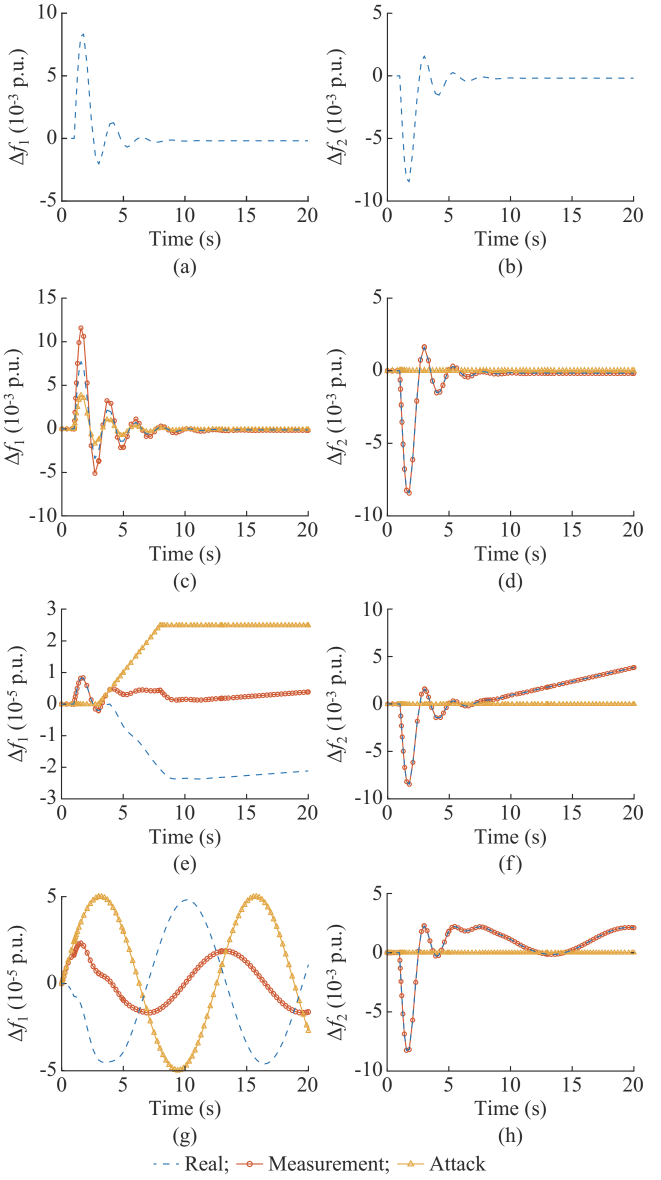


Fig. 6. Frequency deviations of two-area LFC system with WT-PV power generation in area 1 under different attacks on area 1. (a) Δf_1 under normal circumstances. (b) Δf_2 under normal circumstances. (c) Δf_1 under a scaling attack on area 1. (d) Δf_2 under a scaling attack on area 1. (e) Δf_1 under a ramp attack on area 1. (f) Δf_2 under a ramp attack on area 1. (g) Δf_1 under a sine attack on area 1. (h) Δf_2 under a sine attack on area 1.

When the ramp attack is injected into area 2, it has a slope of 0.005 and an upper limit of 0.025, as displayed in Fig. 7(d). As the attack value increases, the real frequency deviation value of area 2 decreases. When the attack value is stable, the real frequency deviation value of area 2 gradually declines. Due to the influence of area 2, as illustrated in Fig. 7(c), the real frequency deviation value of area 1 fluctuates for a while and then keeps falling, which can not reach the stable state. After a sine attack is injected into area 2, which has the amplitude of 0.05 and the frequency of 0.5, as illustrated in Fig. 7(f), the real frequency deviation value fluctuates slightly within a certain range in area 2, then it changes with the period. As shown in Fig. 7(e), due to the effect of the load, the real frequency deviation value oscillates for a short time in area 1, then it fluctuates periodically with the influence of area 2.

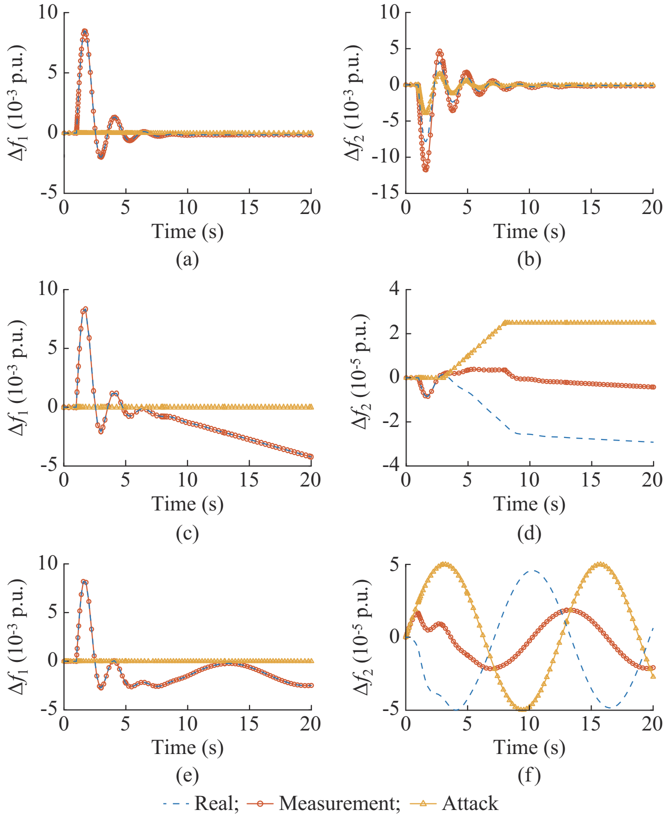


Fig. 7. Frequency deviations of two-area LFC system with WT-PV power generation in area 1 under different attacks on area 2. (a) Δf_1 under a scaling attack on area 2. (b) Δf_2 under a scaling attack on area 2. (c) Δf_1 under a ramp attack on area 2. (d) Δf_2 under a ramp attack on area 2. (e) Δf_1 under a sine attack on area 2. (f) Δf_2 under a sine attack on area 2.

3) Frequency Deviations with WT-PV Power Generation System in Each of Two Areas

Figure 8 indicates the frequency deviations of the two-area LFC system with WT-PV power generation in each of the two areas under different attacks on area 1. Under normal situation, comparing Fig. 8(b) with Fig. 6(b), they are all symmetrical about the *x*-axis, which draws the WT-PV power generation system as the power generation module, and its output value is twice the load value. Likewise, Fig. 8(d) and Fig. 6(d) are also *x*-axis symmetric. Figure 8(f) and (h) and Fig. 6(f) and (h) are symmetrical about the *y*-axis in the first three seconds, then the change trends of real frequency deviation values are the same in the two scenarios, because the attack types are the same. In addition, Fig. 8(a), (c), (e), (g) are the same as Fig. 6(a), (c), (e), (g), respectively, which means that a WT-PV power generation system with appropriate capacity is added to area 2 and it will not affect area 1.

By analyzing the impacts of various attacks on the frequency deviations from different situations, we can draw the following conclusions. Firstly, different kinds of attacks have different effects on the two-area LFC system. Under a slight attack, the system resumes stable operation after a period of fluctuation. However, under a severe attack, excessive frequency oscillations may cause irreversible and dangerous operation trend of the system. Secondly, the WT-PV power generation system affects the dynamic characteristics of the LFC system. In addition, if the WT-PV power generation system with appropriate capacity is added to one area, the other area will not be affected. Thirdly, the two areas influence each other. Under a slight attack, one area returns to stable state after slight fluctuation, the other area is not affected. Under a severe attack, one area cannot reach its original state, and the other area cannot reach its stable state.

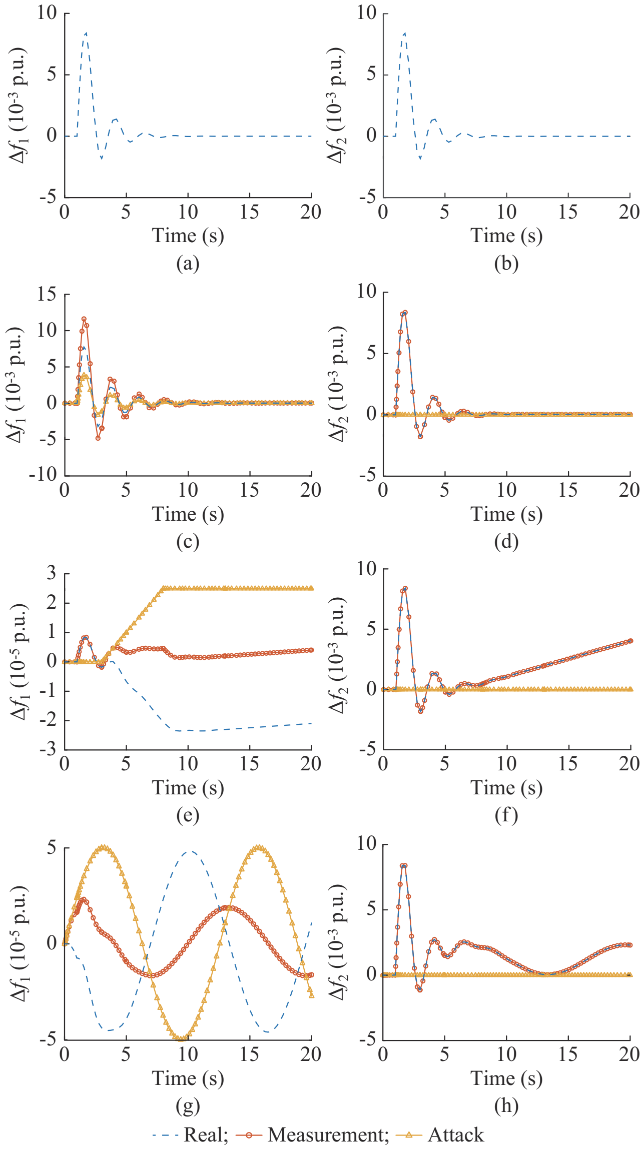


Fig. 8. Frequency deviations of two-area LFC system with WT-PV power generation in each of two areas under different attacks on area 1. (a) Δf_1 under normal circumstances. (b) Δf_2 under normal circumstances. (c) Δf_1 under a scaling attack on area 1. (d) Δf_2 under a scaling attack on area 1. (e) Δf_1 under a ramp attack on area 1. (f) Δf_2 under a ramp attack on area 1. (g) Δf_1 under a sine attack on area 1. (h) Δf_2 under a sine attack on area 1.

B. Test Results of Detection Performance

In order to verify the feasibility of the modified method, the accuracy of three methods for detecting various FDIAs are compared in this subsection. Firstly, the two-area LFC system is constructed on MATLAB/Simulink. Secondly, 24 groups of faults are simulated in the dynamic system. Specifically, typical FDIAs containing scaling attack, ramp attack, sine attack, and hybrid FDIAs including CRAs, SRAs, SSAs, and RSAs are injected in different environments. As shown in Table III and Table IV, the types and the targets of 24 faults are described. Thirdly, the impacts of different attacks on the dynamic system are analyzed. Fourthly, 24000 experimental samples with 10 features including the ACE value, deviation values of measurement frequency, real frequency, attack frequency, power output, and mechanical output of generator and load are obtained from two-area LFC system. Specifically, 6000 experimental samples are obtained from the two-area LFC system without WT-PV power generation; 9000 experimental samples are obtained from the two-area LFC system with WT-PV power generation in area 1; and 6000 experimental samples are from the two-area LFC system with WT-PV power generation in each area. Then, 19200 experimental samples are applied to train the FNN models, and 4800 experimental samples are applied to calculate the accuracy of FNNs for detecting the kinds of FDIAs, which is based on Python platform. Lastly, as demonstrated in Tables V and VI, the performances of four methods for detecting 24 faults by four evaluation indexes are compared.

TABLE III
Type and Target of Typical FDIA

Type	Target	Attack
A_1	Two-area LFC system without WT-PV power generation	Scaling attack on area 1
A_2	Two-area LFC system without WT-PV power generation	Ramp attack on area 1
A_3	Two-area LFC system without WT-PV power generation	Sine attack on area 1
A_4	Two-area LFC system with WT-PV power generation in area 1	Scaling attack on area 1
A_5	Two-area LFC system with WT-PV power generation in area 1	Ramp attack on area 1
A_6	Two-area LFC system with WT-PV power generation in area 1	Sine attack on area 1
A_7	Two-area LFC system with WT-PV power generation in area 1	Scaling attack on area 2
A_8	Two-area LFC system with WT-PV power generation in area 1	Ramp attack on area 2
A_9	Two-area LFC system with WT-PV power generation in area 1	Sine attack on area 2
A_{10}	Two-area LFC system with WT-PV power generation in each area	Scaling attack on area 1
A_{11}	Two-area LFC system with WT-PV power generation in each area	Ramp attack on area 1
A_{12}	Two-area LFC system with WT-PV power generation in each area	Sine attack on area 1

The indexes contain recall (Reca), precision (Prec), and F_1-score, which are based on the confusion matrix. Moreover, the average (Avg) of the values obtained by these three indexes is also calculated. These three indexes are derived from the calculation of true positive (TP), false positive (FP), false negative (FN), and true negative (TN) [32]. In details, the three indexes are defined as:

TABLE IV
TYPE AND TARGET OF HYBRID FDIA

Type	Target	Attack
HA_1	Two-area LFC system without WT-PV power generation	SRAs on area 1
HA_2	Two-area LFC system without WT-PV power generation	SSAs on area 1
HA_3	Two-area LFC system without WT-PV power generation	RSAs on area 1
HA_4	Two-area LFC system with WT-PV power generation in area 1	SRAs on area 1
HA_5	Two-area LFC system with WT-PV power generation in area 1	SSAs on area 1
HA_6	Two-area LFC system with WT-PV power generation in area 1	RSAs on area 1
HA_7	Two-area LFC system with WT-PV power generation in area 1	SRAs on area 2
HA_8	Two-area LFC system with WT-PV power generation in area 1	SSAs on area 2
HA_9	Two-area LFC system with WT-PV power generation in area 1	RSAs on area 2
HA_{10}	Two-area LFC system with WT-PV power generation in each area	SRAs on area 1
HA_{11}	Two-area LFC system with WT-PV power generation in each area	SSAs on area 1
HA_{12}	Two-area LFC system with WT-PV power generation in each area	RSAs on area 1

$$Prec=\frac{TP}{TP+FP} \tag{18}$$

$$Reca=\frac{TP}{TP+FN} \tag{19}$$

$$F_1=\frac{2Prec\cdot Reca}{Prec+Reca} \tag{20}$$

where *Prec* is the overall effectiveness of the diagnostic method; *Reca* is the ability of the diagnostic method to identify positive classes; F_1 is the overall index result of *Prec* and *Reca*; *TP* is the proportion of actual faulty cases that are classified as faulty operating condition; *TN* is proportion of actual normal cases that are classified as normal operating condition; *FP* is to the proportion of actual faulty cases that are classified as normal operating situation; and *FN* is the proportion of actual normal cases that are classified as faulty operating situation

The parameter setting of the FNN training is described in Table VII. The number of neurons in hidden layers, the maximum number of iterations, the penalty factors and the subset of fuzzy logic operators are obtained through grid research method [33].

As illustrated in Tables V and VI, the performances of FNNs, NNs, FPTs, and LSTM under 24 groups of faults are compared. A_1-A_{12} represent the 12 types of faults that the LFC system suffers from typical FDIAs, and HA_1-HA_{12} mean the 12 groups of faults that the LFC system suffers from hybrid FDIAs. Under the typical FDIAs, from a horizontal perspective, the accuracy of FNNs for detecting all groups of attacks is higher than 0.93, which embodies the excellent performance of the improved method, and it has favorable robustness in the face of various input disturbances. In addition, the accuracies of A_4-A_9 are equal to or greater than those of A_1-A_3. This shows that as the WT-PV power generation system is added to the simulation model, the detection accuracy increases slightly, which means that the more obviously the system changes, the higher the accuracy of FNNs for detecting attacks. It reflects the high sensitivity of the improved method. From a vertical perspective, in most cases, the accuracies of FNNs for detecting attacks are higher than those of NNs for detecting attacks, and the accuracies of NNs are even lower than 0.9 in 3 cases. More obviously, the accuracies of FNNs for detecting attacks are more superior than those of FPTs for detecting faults in all situations. Conversely, the detection accuracy of FPTs under most attacks is low and unstable, and there are detection blind spots in A_7. Moreover, the detection accuracy of FNNs is not lower than LSTM networks in most cases, and the overall accuracy is more stable than LSTM networks. Specifically, the average accuracy of LSTM networks in A_8 is 0.88, but the average accuracy of FNNs is not lower than 0.93 in all situations.

TABLE V
PERFORMANCE OF FOUR DETECTION METHODS FOR DETECTING TYPICAL FDIAS IN TWO-AREA LFC SYSTEM

Type	FNN				NN				FPT				LSTM			
	Prec	*Reca*	F_1	*Avg*	*Prec*	*Reca*	F_1	*Avg*	*Prec*	*Reca*	F_1	*Avg*	*Prec*	*Reca*	F_1	*Avg*
A_1	0.94	0.97	0.95	0.95	0.84	1.00	0.91	0.92	0.79	1.00	0.88	0.89	1.00	0.98	0.99	0.99
A_2	1.00	0.87	0.93	0.93	1.00	0.91	0.95	0.95	0.94	0.90	0.92	0.92	1.00	0.98	0.99	0.99
A_3	0.92	0.96	0.94	0.94	0.97	0.90	0.93	0.93	1.00	0.77	0.87	0.88	0.92	1.00	0.96	0.96
A_4	0.91	1.00	0.95	0.95	0.88	1.00	0.93	0.94	0.37	1.00	0.54	0.64	0.97	1.00	0.98	0.98
A_5	0.95	0.96	0.95	0.95	1.00	0.95	0.97	0.98	0.97	0.76	0.85	0.86	0.92	0.96	0.94	0.94
A_6	0.96	0.98	0.97	0.97	0.98	0.96	0.97	0.97	0.88	0.79	0.83	0.83	1.00	0.88	0.94	0.94
A_7	0.97	1.00	0.98	0.98	1.00	0.99	1.00	1.00	0	0	0	0	1.00	0.86	0.92	0.93
A_8	1.00	0.95	0.98	0.98	1.00	0.92	0.96	0.96	1.00	0.85	0.92	0.92	0.78	1.00	0.87	0.88
A_9	0.95	0.98	0.97	0.97	0.93	0.95	0.94	0.94	1.00	0.81	0.90	0.90	0.98	0.83	0.90	0.90
A_{10}	0.97	0.97	0.97	0.97	0.89	1.00	0.94	0.94	0.65	1.00	0.79	0.81	1.00	0.99	1.00	1.00
A_{11}	1.00	0.98	0.99	0.99	1.00	0.93	0.96	0.96	1.00	0.79	0.88	0.89	0.95	1.00	0.97	0.97
A_{12}	1.00	0.92	0.96	0.96	1.00	0.95	0.97	0.97	1.00	0.71	0.83	0.85	1.00	0.93	0.96	0.96

TABLE VI
PERFORMANCE OF FOUR DETECTION METHODS FOR DETECTING HYBRID FDIAS IN TWO-AREA LFC SYSTEM

Type	FNN				NN				FPT				LSTM			
	Prec	*Reca*	F_1	*Avg*	*Prec*	*Reca*	F_1	*Avg*	*Prec*	*Reca*	F_1	*Avg*	*Prec*	*Reca*	F_1	*Avg*
HA_1	0.98	0.99	0.99	0.99	0.97	0.99	0.98	0.98	0.85	1.00	0.92	0.92	0.97	1.00	0.98	0.98
HA_2	0.98	1.00	0.99	0.99	0.90	1.00	0.95	0.95	0.98	0.93	0.95	0.95	0.99	0.98	0.99	0.99
HA_3	1.00	0.96	0.98	0.98	1.00	0.97	0.98	0.98	0.93	0.83	0.88	0.88	0.98	0.96	0.97	0.97
HA_4	0.99	0.99	0.99	0.99	0.96	0.98	0.97	0.97	0.96	0.99	0.97	0.97	1.00	0.97	0.99	0.99
HA_5	0.96	1.00	0.98	0.98	0.98	0.92	0.95	0.95	0.82	0.98	0.90	0.90	0.86	0.99	0.92	0.92
HA_6	1.00	0.98	0.99	0.99	1.00	0.94	0.97	0.97	1.00	0.94	0.97	0.97	0.99	0.97	0.98	0.98
HA_7	1.00	1.00	1.00	1.00	0.99	0.95	0.97	0.97	0.62	0.78	0.69	0.70	0.97	1.00	0.98	0.98
HA_8	0.98	0.98	0.98	0.98	0.99	0.99	0.99	0.99	0.66	0.17	0.27	0.37	1.00	1.00	1.00	1.00
HA_9	1.00	0.98	0.99	0.99	1.00	0.98	0.99	0.99	0.74	0.98	0.85	0.86	0.99	0.86	0.92	0.92
HA_{10}	0.98	0.98	0.98	0.98	0.98	0.99	0.99	0.99	0.93	0.99	0.96	0.96	0.99	0.98	0.98	0.98
HA_{11}	0.97	1.00	0.98	0.98	0.88	0.98	0.93	0.93	0.97	1.00	0.99	0.99	0.98	0.99	0.98	0.98
HA_{12}	1.00	0.97	0.98	0.98	1.00	0.97	0.98	0.98	1.00	0.91	0.95	0.95	0.98	0.98	0.98	0.98

TABLE VII
PARAMETER SETTING OF FNN TRAINING

Parameter	Description	Value
j_1	Number of neurons in the 1st hidden layer	10
j_2	Number of neurons in the 2nd hidden layer	10
j_3	Number of neurons in the 3rd hidden layer	10
γ	The maximum number of iterations	500
α	Penalty factor	0.1
O_1	The 1st operater in fuzzy logic	$Einstein_i$
O_2	The 2nd operater in fuzzy logic	$Lukasiewicz_i$
O_3	The 3rd operater in fuzzy logic	$Algebraic_{sum}$
O_4	The 4th operater in fuzzy logic	$Lukasiewicz_u$
O_5	The 5th operater in fuzzy logic	$Einstein_u$
O_6	The 6th operater in fuzzy logic	Mean
O_7	The 7th operater in fuzzy logic	Min
O_8	The 8th operater in fuzzy logic	Max

Under the hybrid FDIAs, from the horizontal perspective, the accuracy of FNNs for detecting all kinds of attacks is higher than 0.98, and especially under the HA_7, the accuracy reaches 1.00. From the vertical perspective, under most instances, the accuracy of FNNs for detecting attacks is higher than NNs, and the accuracy of NNs is lower than 0.98 in six cases. More obviously, the accuracy of FPTs is lower than FNNs under 11 instances, and the accuracy is only 0.37 under the HA_8. Moreover, the accuracy of LSTM networks is higher than FNNs in only one case. In addition, the accuracy of detecting hybrid FDIAs is mostly higher than that of detecting typical FDIAs. Because a hybrid attack is composed of two typical FDIAs at the same time, different types of FDIAs have different characteristics. When multiple typical FDIAs maliciously attack the LFC system at the same time, the damage to the LFC system is also superimposed. Therefore, the changing features of the LFC system under hybrid FDIAs are more easily captured than that under single typical FDIAs.

As shown in Table VIII, the computational cost of FNNs is significantly less than that of FPTs and LSTM networks. Comparing the computational time of the four methods for detecting typical FDIAs and hybrid FDIAs, in most cases, the latter is longer than the former. In general, the detection accuracy of FNNs in various attack environments and various types of attacks is higher and more stable than NNs, FPTs, and LSTM networks, and the computational cost of FNNs is also significantly lower than that of FPTs and LSTMs. FNNs have better performance than NNs, FPTs, and LSTM networks for detecting the FDIAs in the two-area LFC system with RE generation.

TABLE VIII
COMPUTATIONAL TIME OF FOUR DETECTION METHODS

FDIA	Senario	Time (s)			
		FNN	NN	FPT	LSTM
Typical FDIA	Training	40.80	26.33	242.07	287.79
	Test	0.05	0.04	0.02	1.80
Hybrid FDIA	Training	32.76	29.47	281.38	299.32
	Test	0.04	0.04	0.02	1.89

To demonstrate the scalability of the proposed method, the accuracy of FNNs for detecting typical and hybrid FDIAs on the four-area LFC system is shown in Tables IX and X, respectively. The accuracy of FNNs for detecting typical and hybrid FDIAs is higher than 0.93, which reflects the stability and feasibility of the proposed method. And in most cases, the accuracy is close to be 1, which shows the robustness of FNNs.

VI. CONCLUSION

This paper introduces an improved data-driven method, which is composed of fuzzy logic and NNs. Various types of typical and hybrid FDIAs are defined, including ramp attack, scaling attack, sine attack, SRA, SSA, and RSA. The dynamic model of the multi-area LFC system is set up, and then three simulation scenarios are constructed and developed in MATLAB/Simulink platform. They are LFC system without RE generation, LFC system with RE generation in one area, and LFC system with RE generation in each of two areas.

TABLE IX
Performance of Proposed Method for Detecting Typical FDIAs in Four-area LFC System

Type	*Prec*	*Reca*	F_1	*Avg*
A_1	0.98	1.00	0.99	0.99
A_2	1.00	0.98	0.99	0.99
A_3	0.98	0.97	0.98	0.98
A_4	1.00	0.86	0.92	0.93
A_5	1.00	1.00	1.00	1.00
A_6	1.00	1.00	1.00	1.00
A_7	0.87	1.00	0.93	0.93
A_8	1.00	0.99	0.99	0.99
A_9	0.98	0.99	0.98	0.98
A_{10}	0.99	1.00	0.99	0.99
A_{11}	1.00	0.99	0.99	0.99
A_{12}	0.98	0.99	0.98	0.98

TABLE X
Performance of Proposed Method for Detecting Hybrid FDIAs in Four-area LFC System

Type	*Prec*	*Reca*	F_1	*Avg*
HA_1	0.99	0.98	0.99	0.99
HA_2	0.89	1.00	0.94	0.94
HA_3	1.00	0.98	0.99	0.99
HA_4	1.00	0.97	0.99	0.99
HA_5	0.96	0.98	0.97	0.97
HA_6	1.00	0.97	0.98	0.98
HA_7	0.99	0.97	0.98	0.98
HA_8	1.00	0.95	0.98	0.98
HA_9	0.99	0.97	0.98	0.98
HA_{10}	1.00	0.99	1.00	1.00
HA_{11}	1.00	1.00	1.00	1.00
HA_{12}	0.99	0.98	0.99	0.99

The impacts of different FDIAs on the two-area and four-area LFC systems under three circumstances are analyzed, and a large number of experimental samples with system change are obtained to verify the excellent performance of FNNs. The detection results illustrate higher and more steady accuracy for detecting various FDIAs by FNNs than those by NNs, FPTs, and LSTM networks under most conditions. And the computational cost of FNNs is obviously less than that of FPTs and LSTM networks, which shows the excellent performance of FNNs for detecting FDIAs on LFC system with RE generation. In addition, the accuracy of FNNs for detecting hybrid FDIAs is higher than that of single typical FDIAs, which means that when multiple typical FDIAs maliciously attack the LFC system at the same time, the damage to the LFC system is also superimposed, and the impact on the system is also more serious. Moreover, the improved method has a broad range of applications and relies on historical data to train statistical models and does not require real physical models, which decreases the issues due to "model-reality mismatch".

Future work will consider semi-supervised learning, which can comprehensively use labeled and unlabeled data to generate suitable classification functions, and can detect unknown attacks. In addition, some unique attacks can also be studied such as stealthy attacks and time-delay attacks. Moreover, a more general test system can be simulated based on MATLAB/Simulink platform.

References

[1] Y. Liu, Y. Li, Y. Wang *et al.*, "Robust and resilient distributed optimal frequency control for microgrids against cyber attacks," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 1, pp. 375-386, Apr. 2021.

[2] Y. Wang, Y. Liu, and J. Li, "Deducing cascading failures caused by cyberattacks based on attack gains and cost principle in cyber-physical power systems," *Journal of Modern Power Systems and Clean Energy*, vol. 7, no. 6, pp. 1450-1460, Nov. 2019.

[3] M. U. Usman and M. O. Faruque, "Applications of synchrophasor technologies in power systems," *Journal of Modern Power Systems and Clean Energy*, vol. 7, no. 2, pp. 211-226, Mar. 2019.

[4] M. H. Syed, E. Guillo-Sansano, A. Mehrizi-Sani *et al.*, "Load frequency control in variable inertia systems," *IEEE Transactions on Power Systems*, vol. 35, no. 6, pp. 4904-4907, Nov. 2020.

[5] K. Xiahou, Y. Liu, and Q. Wu, "Robust load frequency control of power systems against random time-delay attacks," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 909-911, Jan. 2021.

[6] H. Zhan, C. Wang, Y. Wang *et al.*, "Relay protection coordination integrated optimal placement and sizing of distributed generation sources in distribution networks," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 55-65, Jan. 2016.

[7] N. Živković and A. T. Sarić, "Detection of false data injection attacks using unscented Kalman filter," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 847-859, Sept. 2018.

[8] 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, Mar. 2019.

[9] M. H. Ansari, V. T. Vakili, B. Bahrak *et al.*, "Graph theoretical defense mechanisms against false data injection attacks in smart grids," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 860-871, Sept. 2018.

[10] J. Yu, Y. Hou, and V. Li, "Online false data injection attack detection with wavelet transform and deep neural networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 3271-3280, Jul. 2018.

[11] 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.

[12] C. Gu, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in AC state estimation," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2476-2483, Sept. 2015.

[13] H. Sedghi and E. Jonckheere, "Statistical structure learning to ensure data integrity in smart grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1924-1933, Jul. 2015.

[14] Y. Chakhchoukh and H. Ishii, "Coordinated cyber-attacks on the measurement function in hybrid state estimation," *IEEE Transactions on Power Systems*, vol. 30, no. 5, pp. 2487-2497, Sept. 2015.

[15] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2218-2234, May 2020.

[16] P. Razmi, M. O. Buygi, and M. Esmalifalak, "A machine learning approach for collusion detection in electricity markets based on nash equilibrium theory," *Journal of Modern Power Systems and Clean Energy*, vol. 9, no. 1, pp. 170-180, Jan. 2021.

[17] R. Senge and E. Hüllermeier, "Fast fuzzy pattern tree learning for classification," *IEEE Transactions on Fuzzy Systems*, vol. 23, no. 6, pp. 2024-2033, Dec. 2015.

[18] H. Zhou, Y. Zhou, J. Hu *et al.*, "LSTM-based energy management for electric vehicle charging in commercial-building prosumers," *Journal of Modern Power Systems and Clean Energy*, vol. 9, no. 5, pp. 1205-1216, Sept. 2021.

[19] J. Wang, X. Chen, F. Zhang *et al.*, "Building load forecasting using deep neural network with efficient feature fusion," *Journal of Modern Power Systems and Clean Energy*, vol. 9, no. 1, pp. 160-169, Jan. 2021.

[20] Q. Zhu, C. Zhang, Y. He *et al.*, "Energy modeling and saving potential analysis using a novel extreme learning fuzzy logic network: a case study of ethylene industry," *Applied Energy*, vol. 213, pp. 322-

333, Mar. 2018.

[21] J. Wang, X. Chen, F. Zhang *et al.*, "Building load forecasting using deep neural network with efficient feature fusion," *Journal of Modern Power Systems and Clean Energy*, vol. 9, no. 1, pp. 160-169, Jan. 2021.

[22] W. H. Allen, A. Rubaai, and R. Chawla, "Fuzzy neural network-based health monitoring for HVAC system variable-air-volume unit," *IEEE Transactions on Industry Applications*, vol. 52, no. 3, pp. 2513-2524, May 2016.

[23] S. D. Kermany, M. Joorabian, S. Deilami *et al.*, "Hybrid islanding detection in microgrid with multiple connection points to smart grids using fuzzy-neural network," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 2640-2651, Jul. 2017.

[24] R. Zhang and J. Tao, "A nonlinear fuzzy neural network modeling approach using an improved genetic algorithm," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 7, pp. 5882-5892, Jul. 2018.

[25] J. Zhu, *Optimization of Power System Operation*. Hoboken: John Wiley & Sons, 2015.

[26] L. Jin, R. Mesiar, and R. R. Yager, "On WA expressions of Induced OWA operators and inducing function based orness with application in evaluation," *IEEE Transactions on Fuzzy Systems*, vol. 29, no. 6, pp. 1695-1700, Mar. 2020.

[27] B. Schweizer and A. Sklar. (1964, Jan.). Associative functions and abstract semigroups. [Online]. Available: https://www. researchgate. net/publication/242607711_Associative_Functions_and_Abstract_Semigroups

[28] S. Admasie, S. B. A. Bukhari, T. Gush *et al.*, "Intelligent islanding detection of multi-distributed generation using artificial neural network based on intrinsic mode function feature," *Journal of Modern Power Systems and Clean Energy*, vol. 8, no. 3, pp. 511-520, May 2020.

[29] D. Li, Y. Wang, T. Song *et al.*, "An adaptive policy evaluation network based on recursive least squares temporal difference with gradient correction," *IEEE Access*, vol. 6, pp. 7515-7525, Feb. 2018.

[30] Y. Wang, D. Gan, N. Zhang *et al.*, "Feature selection for probabilistic load forecasting via sparse penalized quantile regression," *Journal of Modern Power Systems and Clean Energy*, vol. 7, no. 5, pp. 1200-1209, Sept. 2019.

[31] C. Chen, K. Zhang, K. Yuan *et al.*, "Novel detection scheme design considering cyber attacks on load frequency control," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, pp. 1932-1941, May 2018.

[32] M. Li, D. Yu, Z. Chen *et al.*, "A data-driven residual-based method for fault diagnosis and isolation in wind turbines," *IEEE Transactions on Sustainable Energy*, vol. 10, no. 2, pp. 895-904, Apr. 2019.

[33] D. Deng, X. Chen, R. Zhang *et al.*, "XGraphBoost: extracting graph neural network-based features for a better prediction of molecular properties," *Journal of Chemical Information and Modeling*, vol. 61, no. 6, pp. 2697-2705, May 2021.

Ziyu Chen received the B.S. degree in electrical engineering from Guangdong University of Technology, Guangzhou, China, in 2017. She is currently pursuing the Ph.D. degree with the School of Electric Power Engineering, South China University of Technology, Guangzhou, China. Her current research interests include cyber-physical-social systems, operation and control of smart energy system, and cyber attack detection.

Jizhong Zhu received the B.S., M.S., and Ph.D. degrees in electrical engineering from Chongqing University, Chongqing, China, in 1985, 1987, and 1990, respectively. His work experience includes Chongqing University, Chongqing, China; Brunel University, Brunel, U.K.; National University of Singapore, Singapore; Howard University, Washington DC, USA; ALSTOM Grid Inc, Redmond, USA; Electric Power Research Institute of China Southern Power Grid Co., Ltd., Guangzhou, China; China Southern Power Grid, Guangzhou, China. He is a Fellow of IEEE and a Professor at the School of Electric Power Engineering, South China University of Technology, Guangzhou, China. His research interests include power system operation and control, smart grid, microgrid, virtual power plant, electric vehicle, renewable energy application, and integrated smart energy system.

Shenglin Li received the B.S. and M.S. degrees both from Shanghai University of Electric Power, Shanghai, China, in 2016 and 2019, respectively. He is currently working towards the Ph.D. degree with the School of Electric Power Engineering, South China University of Technology, Guangzhou, China. His current research interests include energy management of renewable energy microgrids as well as energy trading.

Yun Liu received the B.Eng. (First Class Hons.) and Ph.D. degrees from the College of Electrical Engineering, Zhejiang University, Hangzhou, China, in 2011 and 2016, respectively. His work experience includes the University of Central Florida, Orlando, USA; Nanyang Technological University, Singapore; and Shenzhen University, Shenzhen, China. He is currently an Associate Professor with the School of Electrical Power Engineering, South China University of Technology, Guangzhou, China. His research interests include power system stability analysis, microgrid, integrated energy systems and distributed control and optimization.

Tengyan Luo received the B.S. degree in electrical engineering and automation from Zhengzhou University, Zhengzhou, China. She is currently working towards the M.S. degree in the School of Electric Power, South China University of Technology, Guangzhou, China. Her current research interests include renewable energy and integrated energy systems.