Electrical Power and Energy Systems 132 (2021) 107151

Contents lists available at ScienceDirect

International Journal of Electrical Power and Energy Systems

journal homepage: www.elsevier.com/locate/ijepes

Time-frequency based cyber security defense of wide-area control system for fast frequency reserve☆

Wei Qiu [a,b], Kaiqi Sun [b,*], Wenxuan Yao [a], Shutang You [b], He Yin [b], Xiaoyang Ma [d], Yilu Liu [b,c]

[a] Hunan University, 410082 Changsha, China
[b] Department of EECS, University of Tennessee, Knoxville, 37996 TN, USA
[c] Oak Ridge National Laboratory, Knoxville, 37830 TN, USA
[d] Sichuan University, 12530 Chengdu, China

ARTICLE INFO

Keywords:
Energy storage
WAMS-based FFR system
Time-frequency domains
Dual-frequency scale convolutional neural networks
Spoofing attacks

ABSTRACT

Global power systems are transiting from conventional fossil fuel energy to renewable energies due to their environmental benefits. The increasing penetration of renewable energies presents challenges for power system operation. The efficiency and sufficiency of responsive reserves have become increasingly important for power systems with a high proportion of renewable energies. The Fast Frequency Reserve (FFR), especially the Wide-area Monitoring System (WAMS)-based FFR, is a promising and effective solution to secure and enhance the stability of power systems. However, cyber security has become a new challenge for the WAMS-based FFR system. Cyber attacks on the FFR control system may threaten the safety of power system operation due to the rapid power controllability requirement of FFR. To address this problem, a time-frequency based cyber security defense framework is proposed to detect the cyber spoofing of synchrophasor data in WAMS-based FFR control systems. This paper first introduces the Continuous Wavelet Transforms (CWTs) to decompose spoofing signals. Then, the Dual-frequency Scale Convolutional Neural Networks (DSCNN) is proposed to identify the time-frequency domains matrix from two frequency scales. Integrating CWTs and DSCNN, an identification framework called CWTs-DSCNN is further proposed to detect the spoofing attacks in the WAMS-based FFR system. Multiple experiments using the actual data from FNET/GridEye are performed to verify the effectiveness of the framework in securing WAMS-based FFR systems.

1. Introduction

The transition of global energy from fossil fuel energy to renewable energy has significantly accelerated in the past decade [1,2]. According to 2020 Renewable Global Status Report, the newly installed capacity of renewable energies is record-breaking in 2019, growing by more than 200 gigawatts (GW), which is the largest installation capacity increase in history [3]. Additionally, as research and development efforts and energy policies in almost all countries are increasingly focusing on renewable energy development, it is clear that the renewable penetration in power systems will continually increase in the foreseeable future [4].

Due to the physical characteristics of renewable energies, renewable generation is usually integrated into power systems through Grid-connected Converters (GCCs) [5]. As is well known, system inertia is provided by generators and motors rotating at the same frequency, which forms the power grid frequency [6,7]. However, the GCC connection decouples generator rotors to power grids, and some even do not have mechanical rotors. Therefore, most renewable energies can not provide the necessary grid services [8]. With the increasing penetration of renewable energies, the system inertia decreases inevitably. When an event occurs (e.g., generator trip or load loss), the stability of the power system with a high proportion of renewable energies will be more vulnerable. For example, the Rate of Change of Frequency (RoCoF) and the frequency deviation would be larger for the same amount of power imbalance, and finally leads to the tripping of protection relays [9]. As the generation mix changes, maintaining the system frequency at acceptable levels becomes a thorny issue [10].

To handle the emergency operating situations of low inertia systems, Fast Frequency Reserve (FFR) has received much attention in recent

☆ Postgraduate Scientific Research Innovation Project of Hunan Province under Grant CX20200426.
* Corresponding author.
E-mail address: ksun8@utk.edu (K. Sun).

https://doi.org/10.1016/j.ijepes.2021.107151
Received 6 December 2020; Received in revised form 15 February 2021; Accepted 24 March 2021
Available online 11 May 2021

years [11,12]. According to the definition by the North American Electric Reliability Corporation (NERC), FFR is designed to provide a fast power response to changes in the measured or observed frequency during a frequency excursion event [13]. In the past, the inertial response from synchronous generators is the dominant FFR in the system. With the conventional generator retired and replaced by renewable energies, system operators proposed higher response requirements [14]. In the frequency response requirement of the California Independent System Operator (CAISO), FFRs need to act within the first few seconds. The frequency response of synchronous generators cannot meet the operating requirement [15,16]. The FFR provided by energy storage devices and fast-responding controls from renewable energies, such as batteries, flywheels, and kinetic energy extraction from Wind Generators (WGs), has become the mainstream in recent years [17,18].

Due to its fast response capability to the frequency deviation, the FFR has been widely recognized as the primary response to the frequency excursion of low-inertia systems. Some frequency regulation methods based on the FFR response have been studied, including using the rotating kinetic energy from WG [19,20], and extracting energy stored in DC links [21]. The demand-side response has also been studied, such as the aggregation of refrigerators [22], smart loads [23], and PV panel control [24].

So far, most control methods for FFRs are based on local frequency measurement. Due to its dependence on the geographical distribution of renewable resources and grid infrastructure, the location of renewable generation is typically distributed non-uniformly [25]. The local measurement-based FFRs cannot exactly match the power requirement and FFRs response. As a result, the output from the FFRs may not improve frequency performance and even cause inter-regional power oscillations [26]. With the advancement of the phasor measurement unit (PMU) in accuracy and the reporting rate, wide-area monitoring system (WAMS) provides system operators with an unprecedented way to monitor and control power systems. In [27], a WAMS-based FFR control system is presented, which uses real-time data from PMUs to determine the required responses and allocate them to FFRs. Compared to the conventional FFR control, this WAMS-based control could realize the coordination and optimization of FFR in the system, improving the system stability. With the increasing need of FFRs, the WAMS-based FFR is a promising solution for system stability enhancement.

However, the data security of PMUs has always been vulnerable as evidenced by the increasing reported cases of cyber attacks. Owing to their operating principle and communication methods, PMUs are easy to be penetrated [28]. In various attack methods, the network-based false data injection (NFDI) attack may seriously influence the authenticity of data, causing malfunction of FFRs, which is even worse than the case without FFRs. Considering the fast response capability of FFRs, the risk of the reverse direction regulation of FFRs could be a potential disaster to the system stability. Therefore, cyber-attack detection becomes essential for the FFR response.

Due to its importance, there has been some research on the defense against power grid attacks. In [29], the hijacking attacks are detected in DC microgrids using the distributed screening method. The attack on the AC/HVDC interconnected system has also been studied in [30] through manipulating the system measurements of frequencies. However, these methods require the values of other parameters of the circuit, such as the current, to achieve accurate detection. This limits its application to the FFR control circuits. Meanwhile, from the energy perspective, the attack will deplete the available energy, including the batteries and photovoltaic [31]. A two-stage robust optimization is proposed to mitigate the uncertainties and adverse impacts caused by NFDI attacks in [32].

For the attack detection in frequency control systems, some research has also investigated the defense strategies for the cyber attack. [33] develops an approach based on a novel stochastic unknown input estimator to detect the attack in the AGC. The proposed method does not need information about real-time load changes, which significantly improve state estimation accuracy. Based on the state estimation accuracy, [34] analysis four different attack strategies and their impact on load frequency control. Based on the analysis results, a detection method based on a Multilayer perception classifier-based approach is proposed to extract the differences between the normal signal and compromised signals. Based on the passive fault attenuation principle, [35] design a new distributed cyber-attack-tolerant frequency control to improve the frequency performance and the tolerance under cyber attack. [36] develops a new virtual inertia control strategy that adopting the virtual damper to enhance the conventional virtual inertia control so that improve the frequency response performance such as frequency nadir and oscillation under the time delay attacks. One common feature of these attacks is the modification of the measurement data. In the NFDI attack, such measurements are tampered behaviors that can be considered as a replay attack. The replacement signal in these attacks can be very similar to the raw measurement, bringing challenges for accurate attack detection.

Depending on the robustness of attack detection, cyber security defense methods can be divided into model-based methods and model-free methods. Model-based methods usually establish state equations to detect the attack [37]. Changes in measured values will cause changes in state variables. Then, attacks can be detected based on the measurement residual vector or state variables [38]. These model-based methods build equations based on the system structure. Therefore, the configuration information on the previous state is needed, which sacrifices its generality and adaptability.

Model-free methods include traditional machine learning methods and deep learning methods [39]. They also belong to data-driven methods, which make full use of the PMU data in the FFR control system. For example, the Random Forest Classification (RFC) and gcForest are used to detect the spoofing attack by extracting the spatio-temporal characteristics from the synchrophasor data [40,41]. Additionally, the data authentication method is proposed to detect the data spoofing based on ensemble empirical mode decomposition (EEMD) and back propagation (BP) neural network [42]. These methods are based on the frequency domain features of the signal, because the frequency domain information is considered to be consistent during a short time [43]. However, the period of this frequency information retention is not considered. In [44], the support vector machine is introduced for spoofing events recognition, and the handcrafted correlation vectors are designed for detecting spoofing attacks. However, the time domain-based recognition method is only applicable when the shape of the attack differs from the original measurement value. The above model-free methods either only contain frequency information or only contain time domain information, resulting in an insufficient response to complex attacks. Meanwhile, the simulated data is used in some research. For example, the intentional injections of false synchrophasor measurements detection method is verified based on the IEEE 39-Bus system [45]. Compared with the simulated data and the actual data, the components such as the noise level and frequency components are different. Massive measurement data increases the demand for deep learning methods, which have strong feature extraction capabilities.

Considering the big data in WAMS and the fast response requirement of FFR application, deep learning methods have been introduced for attack detection. In [46], the deep autoencoder is deployed to detect the data manipulation attacks, assuming that the data packets of PMU data can be modified. Besides, a recurrent neural network is proposed to identify the replaced false data in DC microgrids [47]. Nevertheless, the recurrent network is only suitable for the data with a certain trend, while synchrophasor measurement data is often random, especially frequency measurement values. Therefore, the convolutional neural networks (CNN), longshort-term memory (LSTM), and SVM are combined to for detecting tampering attacks using the raw signals in [48], which also demonstrated the profound feature extraction capabilities of deep learning. However, this combination makes this method very complicated and difficult to train. It can be seen from the results of the existing research that the optimized input space is worthy of further mining to

improve the attack detection performance in the FFR control system, so that the response speed can be guaranteed and the FFR control reliability can be improved.

To increase the amount of input information and improve the performance of cyber-attacks detection, a cyber-security defense method is proposed in the WAMS-based FFR control systems. The proposed method includes the following innovations.

1. To extract the information of the attack signal from multiple scales in the WAMS-based FFR control system, the Continuous Wavelet Transforms (CWTs) is applied to transform the spoofing signal and obtain features from the time and frequency domains to enhance feature diversity.
2. To enhance the attack detection ability in the WAMS-based FFR control system, the Dual-frequency Scale CNN (DSCNN) is proposed to process the input data from two frequency scales. This scaling feature improves the detection ability of the spoofing attack.
3. A spoofing attack identification framework of synchrophasor data is developed based on the CWTs and DSCNN. Particularly, the hand-crafted feature design steps can be avoided.
4. Importantly, the time-sensitivity experiment of the spoofing attack detection is first performed in this paper. Compared with some deep learning and advanced attack detection methods, the experimental results verify that the proposed CWTs-DSCNN framework has higher accuracy and better robustness.

The main contribution of this paper is the proposed CWTs-DSCNN, which provides a rapid and reliably cyber security defense mechanism for the WAMS-based FFR control system. The proposed method breaks through the speed and accuracy limitations of the traditional detection methods, significantly improving the operating security of the WAMS-based FFR control system. Additionally, the proposed method has been evaluated with actual synchrophasor data from the Western Interconnection (WECC) system, which verified its practical value in the WAMS-based FFR control system.

The rest of the paper is organized as follows. Section 2 describes the potential impact of the spoofing on the power system. Section 3 presents the time-frequency based signatures extraction using CWTs. And the proposed DSCNN is introduced in Section 4. Next, the proposed CWTs-DSCNN framework is listed in Section 5. Different experiments are conducted in Section 6. Finally, the results and conclusion are discussed in Section 7.

2. The WAMS-based FFR control system under cyber attack

To demonstrate the impact of the attack on FFR control, the control framework of the WAMS-based FFR control system is first introduced, as shown in Fig. 1, where f_{ref} is the nominal frequency, $f_{local-measurement}$ is the measured frequency from Local PMU, f, θ, and V are measured frequency, angle, and voltage, respectively. $\Delta\theta$ is the phase angle difference during pre-disturbance and post-disturbance steady states, $\Delta P_{order-\theta}$ is the power order calculated from the transient stability control in remote fast response controller, $\Delta P_{order-f}$ is the power order calculated from the frequency response control in remote fast response controller, $\Delta P_{order-FFRi}$ is the power order for controlling i^{th} FFR output, $\Delta P_{order-flocal}$ is calculated from the frequency response control in local fast response controller, the ΔP_{FFR-op} is operating output of FFR, ΔP_{FFR} is the power output of FFR after control, $\Delta P_{FFR-max}$ is the power output max of the FFR and k_{FFR} is the response droop coefficient of FFR. The corresponding working process can be described as:

1. *Step*1: The frequencies, phase angles and voltages in different buses are measured by PMUs. Then, the PMUs will send the data to the

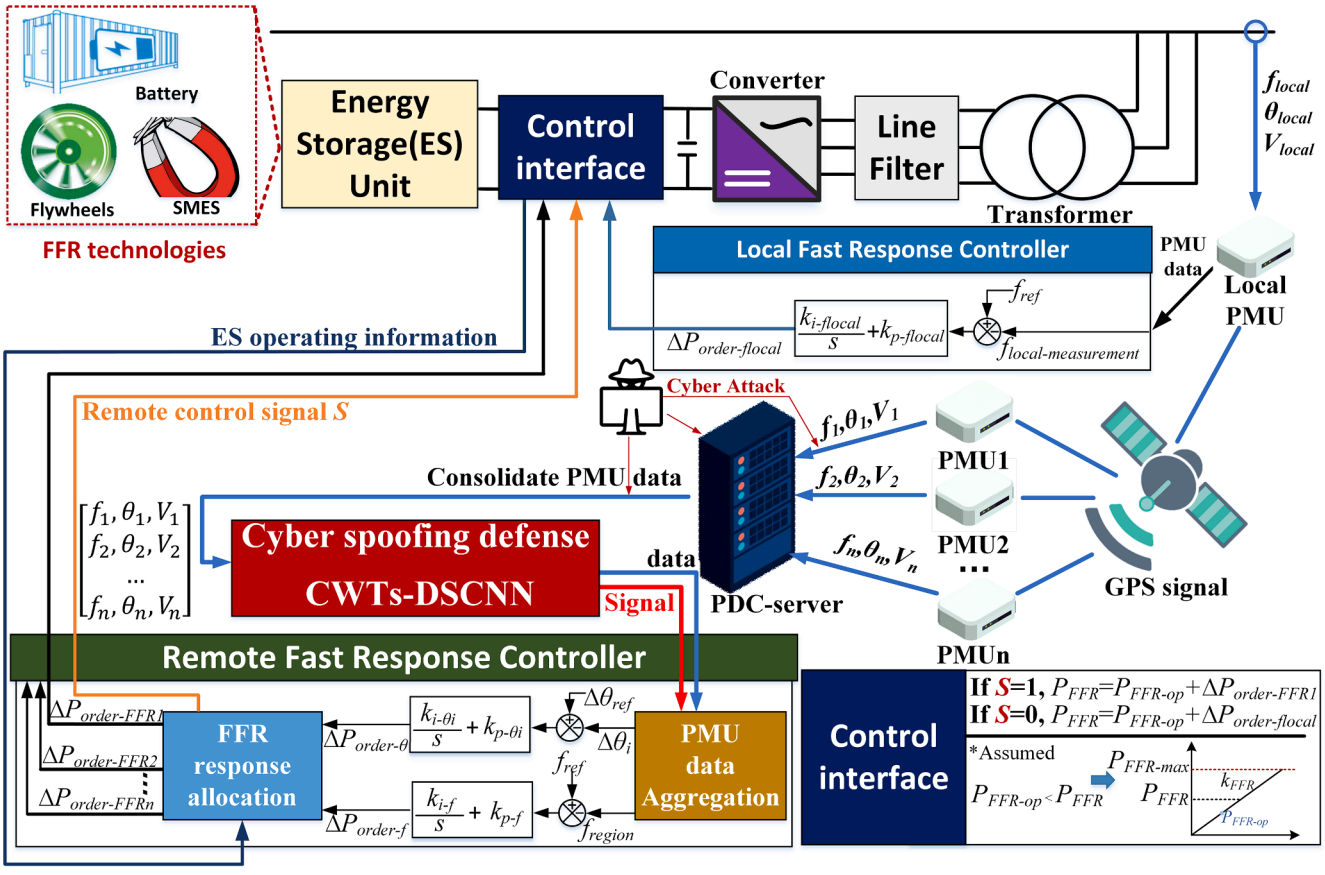

Fig. 1. The control framework of the WAMS-based FFR control system.

Phase Data Concentrators server (PDC-server) via communication protocol IEEE C37.118 [49].

2. *Step*2: After receiving the data packet, the PDC-server will send the consolidate PMU data to remote fast response controller (RFRC) for FFR control. In the RFRC, two control strategies are typically adopted: frequency response control and transient stability control. The frequency response control will aggregate all measured frequencies from PMUs and calculate the power demand of the system by the proposed control strategy (in Fig. 1, the basic frequency droop control strategy is adopted, and other advanced control strategies are also compatible). The transient stability control aims at mitigating the power oscillation on the AC intertie between two areas. The transient stability control is based on the phase angle measured from PMUs. According to the $\Delta\theta$ values on both ends of the AC intertie, the transient stability control will calculate the power requirement of the system.
3. *Step*3: The calculated power demand $\Delta P_{order-f}$ and $P_{order-\theta}$ will be sent into FFR response allocation. The FFR response allocation will allocate the power demand to every FFR according to the proposed advanced allocation strategy.
4. *Step*4: The allocated power order to the FFR will be sent to the control interface of FRR. Meantime, the remote control signal *S*will also be sent to the control interface. If the control interface received the remote control signal, the FFR will adopt the allocated power order from remote fast response controller. Otherwise, the local power order that generated from local fast response controller will be adopted as the control order. In the WAMS-based FFR control system, the priority of the remote fast response controller is higher than the local fast response controller. The local fast response controller will be a backup in case of communication lost.

As shown in Fig. 1, the response of the WAMS-based FFR control system is mainly based on the frequency difference between PMU measurement points. Therefore, frequency data measured from PMUs play a decisive role in the WAMS-based FFR control. However, owing to the vulnerability of the communication protocol, PMUs are easily attacked by cyber attackers. This has been verified by some cyber-attack events reported in recent years [50,51]. Owing to the serious consequences that could be caused by the impaired FFR response, the WAMS-based FFR control system is becoming increasingly attractive to cyber attackers. In Fig. 1, the attack can be targeted at the data transmission between PMUs to the PDC server or between the PDC server to RFRC. Once PMUs are maliciously penetrated by cyber attackers, the fake frequency data will lead to the incorrect calculation of power demand and the wrong response of FFRs.

To illustrate the impact of a cyber attack on the WAMS-based FFR control system, a comparison study is performed on a simplified system. Fig. 2 shows a configuration of the simplified WAMS-based FFR control system. Here, the PMU measures the frequency and send data to PDC, Then, PDC sends the data to the frequency response controller of FFR. The FFR power output will follow the power order calculated from frequency response controller. Before $t = 3$ s, the power output of the FFR is 0 MW. At $t = 3$ s, the frequency data measured from PMU is spoofed in a cyber attack. The frequency response of FFR after this cyber attack event is shown in Fig. 3.

Fig. 3 shows the frequency comparison and FFR power output comparison with and without the cyber attack. As can be seen from Fig. 3, when the spoofing attack data is injected into the PMU, the FFR is activated due to the frequency deviation brought by spoofing attack data. The FFR starts to extract power from the system to its ES unit, trying to reduce to the system frequency deviation. However, since the frequency data that FFR followed has been spoofed, the system frequency is decreased to below 60 Hz. At $t = 7s$, the cyber attack ends, the frequency value sends to FFR is changed from spoofing attack data to the actual system frequency measured by PMUs. Due to the large frequency deviation between the expected and actual values at $t = 7s$, the power direction of FFR changes rapidly to provide power support. It also can be seen from Fig. 3(a) that the system frequency has also dropped more than 0.5 Hz due to the long duration of the spoofing attack. Some electric

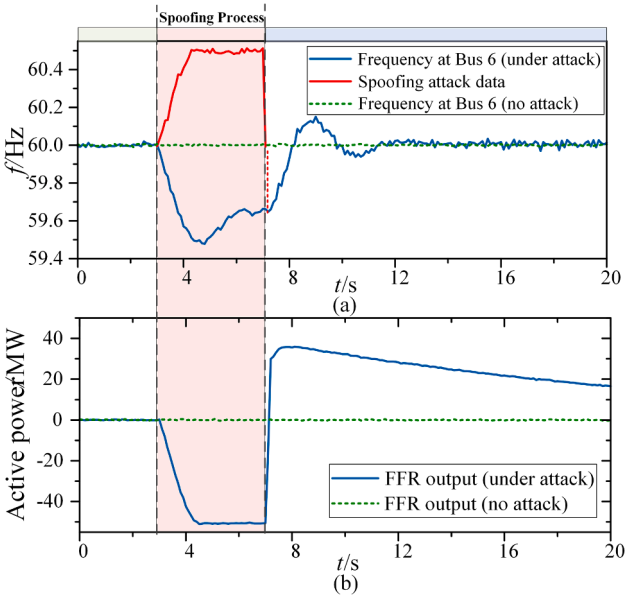

Fig. 3. The frequency response of the simplify WAMS-based FFR control system under cyber attack. (a) Frequency comparison in system. (b) Power output comparison of FFR.

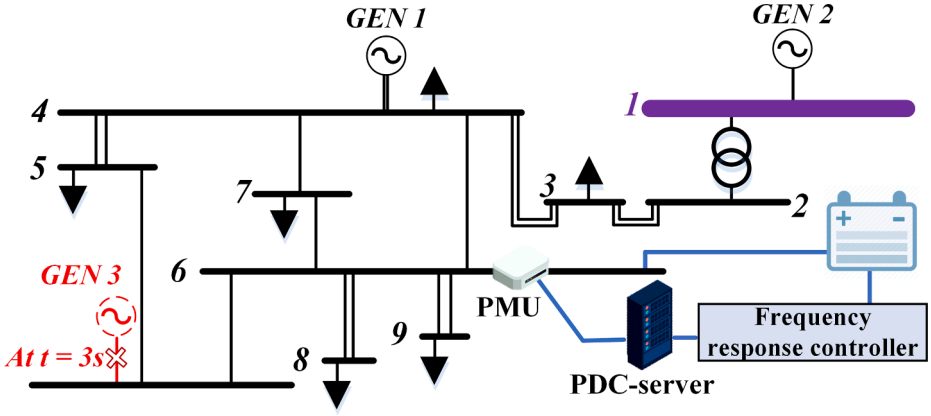

Fig. 2. The architecture diagram of a simplify WAMS-based FFR control system embedding in a test system.

equipment and loads may trip under this frequency. Thus, attack detection is important to mitigate the effect of cyber attacks in WAMS-based FFR control systems.

As shown in Fig. 1, with the proposed attack identification method, the spoofing attack data could be detected rapidly. Then a signal can be sent to the remote fast response controller for stopping the FFR response or activating other recovery strategies to eliminate the frequency deviation. Next, the proposed cyber security defense method will be introduced in detail below.

3. Time-frequency based signatures extraction for spoofing data

3.1. Data detrending

The objective of this section is to detect the source ID cyber spoofing from multiple PMU units. The definition of the source ID cyber spoofing is as follows. Denoted the vector $S_i = \{s_{i,1}, s_{i,2}, \ldots, s_{j,n}\}$ as the measurement data in the i-th PMU in the time 1to$n$. For any unknow synchrophasor data segment $S_s = \{s_1, s_2, \ldots, s_s\}$where $1 \leqslant s \leqslant n$, the source ID cyber spoofing will happen when the data in $S_i$is replaced by $S_s$with a certain time window of the same length [52]. It also should be notable that the playing back and scale attacks can be seen as special cases of source ID spoofing attacks.

The synchrophasor data from WAMS-based FFR control system has a common data trend, which does not contain useful information for attack detection. Before the signatures are extracted, the data preprocessing is necessary to remove this redundant information.

In this paper, the frequency data is selected as verification data for method validity. As shown in Fig. 4, the frequency data from three locations have the same main trend. The difference is the deviation of the frequency change. Actually, the main trend can be regarded as the DC component due to the very small change rate. To remove the main trend, a high pass filter is used in the data preprocessing process.

After that, the synchrophasor data stream is divided into time windows of a 320-point length to facilitate signature extraction, where the sampling rate is 10 Hz.

3.2. Time-frequency signature extraction using CWT

Since the cyber spoofing of WAMS-based FFR control system is secretive, efficient identification methods are required to allow continuous detection. Here, the Continuous Wavelet Transforms (CWTs) is applied to the detrended synchrophasor data. Compared with some advanced data spoofing detection methods, such as the FFT-ANN [43] and the support vector machine [44], only the frequency or the handcrafted statistical features are used, which is usually insufficient to fully describe the characteristics of the input signal because the single statistical feature often only contain information of a specific aspect. The motivation of using the continuous wavelet transforms (CWTs) is to extract features from both the time and frequency domains and improve the performance of the data spoofing detection [53]. Compared with the FFT method, which only gets the frequency domain information of spoofing data, the advantage of CWTs is that it can obtain richer information in the spatio-temporal dimension.

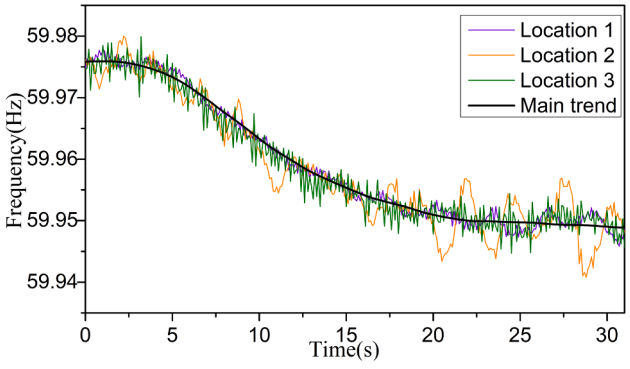

Fig. 4. The measurement synchrophasor data in three locations.

Given the detrended data as $s(t)$, the CWT of $s(t)$ is defined as the convolution calculation method, which can be expressed as

$$S(a,\tau) = \int_{-\infty}^{+\infty} s(t)\frac{1}{\sqrt{|a|}}\psi^*\left(\frac{\tau - t}{a}\right)dt \quad (1)$$

where $a$is the scale factor, which is used to control the signal to be zoomed in or out by changing the value. $\tau$is the time shifting factor. $\psi(t)$and $\psi^*(t)$are the mother wavelet and its complex conjugation, respectively. The time and frequency resolution of CWTs is determined by the wavelet $\psi(t)$.

The output of CWTs is the complex valued matrix. To facilitate the identification of the cyber spoofing signal, the complex valued matrix is further transformed into a power spectrum, which is calculated as

$$E_{cwt}(p,q) = |S(a,\tau)| \quad (2)$$

where the $p$and q are the dimension of the E_{cwt}.

According to the uncertainty principle of signal processing, the time and frequency resolution always contradict each other. In practice, it is hoped that the time resolution is better at high frequencies, and the frequency resolution is better at low frequencies. In CWTs, the mother wavelet $\psi(t)$and the scale factor determine the resolution in different frequency bands. To select the suitable parameters, three different mother wavelet functions, including the complex Gaussian wavelets (Cgau8), Morlet wavelet, and Mexican hat wavelet, are used to show the effect of signal analysis. It should be noted that these three types of mother wavelet functions are selected after the preliminary screening of seven types of mother wavelet functions, which the other four wavelet functions are complex morlet, shannon, frequency B-spline, and Gaussian derivative wavelets. The wavelet functions with relatively low decomposition results are eliminated. The results of CWTs under different wavelet functions are shown in Fig. 5.

The scale factor is optimally selected from multiple candidate sets for a reasonable comparison.

As shown in Fig. 5 (a), the spoofing area occurs between 1.5s to 12s. The results from Fig. 5 show that they contain higher frequency components (higher than 3 Hz) when $t \leqslant 15s$. However, the high frequency components disappear after 16s for the Mexican hat wavelet, which means it has lower time resolution in high frequency bands. In the low frequency bands between 0 to 2 Hz, the details of Cgau8 and Morlet are obvious. It means that they have higher frequency resolution in the low frequency bands. The above analysis shows that the Cgau8 and morlet wavelets performers better. When observing from the frequency axis in Fig. 5(b) and (c), more frequency points are located during 4 to 5 Hz. There are three frequency points during 4 to 5 Hz in Fig. 5(c), and only two frequency points for Fig. 5(b) during 4 to 5 Hz. This means that the Cgau8 has lower frequency resolution and better time resolution in high frequency compared with Morlet wavelet. Therefore, the Cgau8 is selected as the final mother wavelet in CWTs. At this time, the scale factor is selected empirically as $2f_cL/L!$, where $f_c = 0.7$Hz is the center frequency of Cgau8, $L = 320$is the length of each sample.

To show the effectiveness of CWTs for analysing the cyber spoofing data, the comparison between normal and spoofing data is presented in Fig. 6. In Fig. 6(c), the data of (a) is spoofing by the data from an unknown source. As shown in Fig. 6 (b), it mainly contains some low frequency components which are lower than 1 Hz. However, when the data is spoofed in Fig. 6 (c), some frequency components that are higher than 1.5 Hz can be observed, as depicted in Fig. 6(d). Moreover, it can be seen from Fig. 6(c) and (d) that the duration is close to the actual spoofing time. It should be noted that the length of the spoofing area can be changed so the attack would be more invisible. Based on the CWTs, the

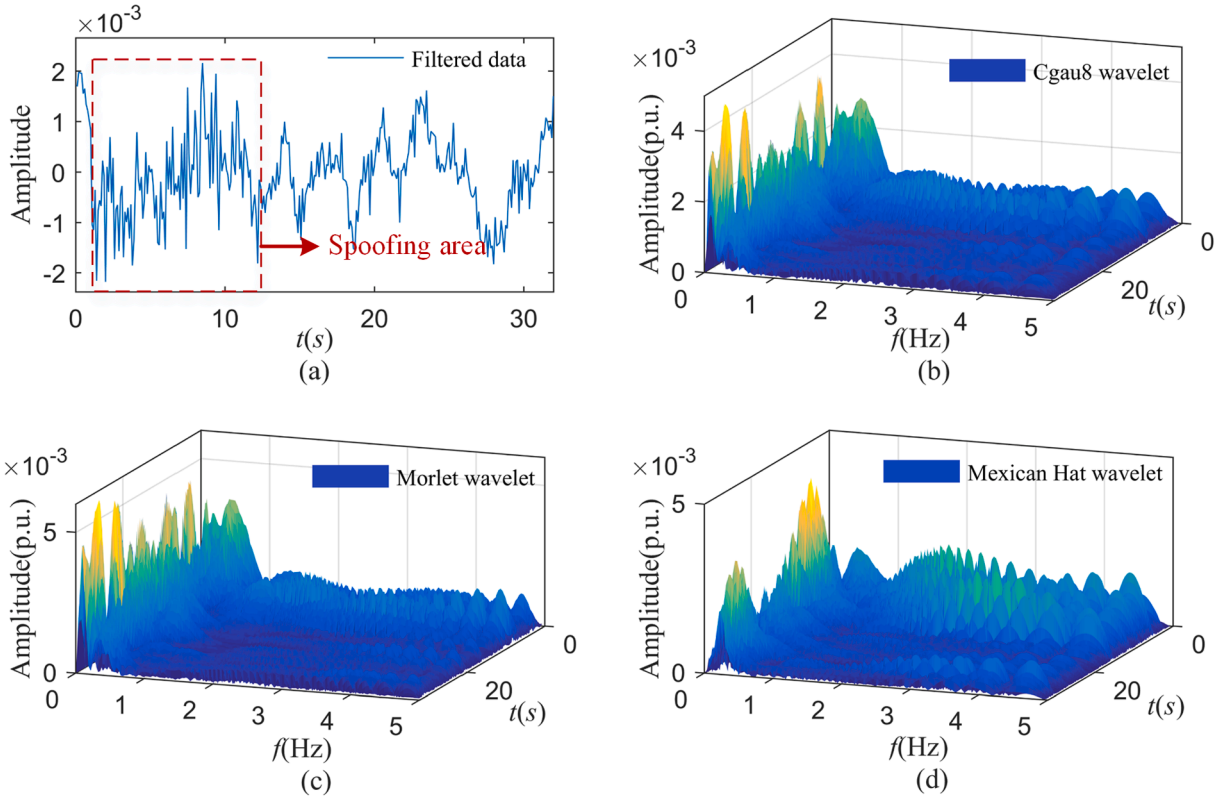

Fig. 5. The CWTs of the spoofing data using three different mother wavelet functions. (a) the spoofing data, (b) the complex Gaussian wavelets with level 8, (c) the Morlet wavelet, (d) the Mexican hat wavelet.

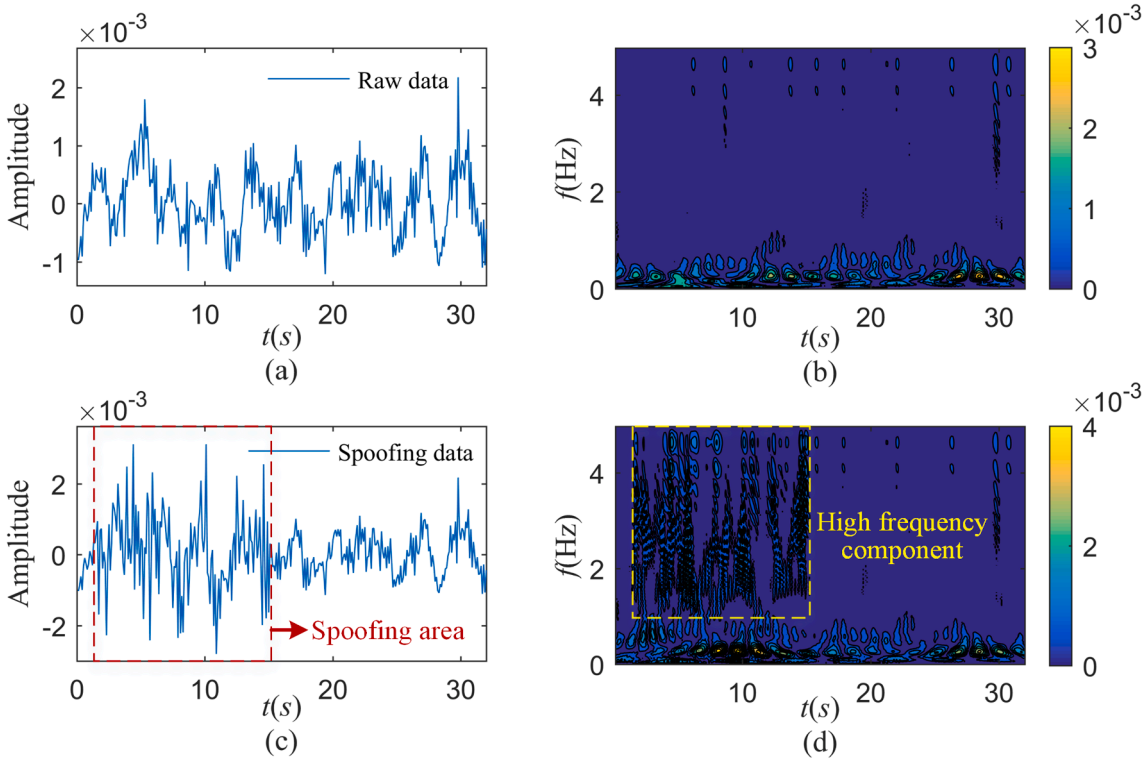

Fig. 6. The time-frequency signatures of the normal and spoofing data. (a) the normal data, (b) the CWT of normal data, (c) the spoofing data, (d) the CWT of spoofing data.

characteristics of cyber spoofing can be observed from the time and frequency domains. Using the differences between the data from the WAMS-based FFR control system, the accurate classifier can then be applied to identify spoofing attacks.

4. Cyber spoofing detection using Dual-frequency Scale CNN

WAMS systems usually have hundreds to thousands of synchrophasor measurement Units. Therefore, it is necessary to use the big data processing method to defend against cyber spoofing. CNN has been developed to learn useful information from massive input data. Compared with some classic machine learning methods, such as ANN, it has higher computing requirements but also higher efficiency [54]. However, its performance suffers from the single convolution method and redundancy. To overcome this problem, this paper proposed a novel Dual-frequency Scale CNN (DSCNN) to improve the calculation efficiency.

4.1. Basic structure of CNN

Generally, CNN structure consists of multiple components, including the convolutional, pooling, and classification layers. The convolutional and pooling layers can be alternated or stacked to form a multilayer network structure [55]. And the classification layer is always at the end of the CNN.

As the name indicates, the signatures of the time-frequency matrix are transformed by the convolutional layer. This layer mainly includes convolution operations and parameter sharing. The diversity of signatures depends on the kernel size *k*and the number of channels of the convolutional layer. However, only one kernel size can be set for each layer, which will lead to single characteristics and pass a single message to the next layer. For example, if the input data is calculated by a convolution kernel sized 3 times 3, the output of this layer would be some local features due to its small size. Therefore, this layer mainly determines the performance of CNN.

The pooling layer is used to filter the extracted signature information while reducing the data dimension. If too many signatures are filtered in each pooling layer, it may cause under-fitting. In contrast, if only a small part of the information is filtered, it will cause overfitting. Normally, the parameters of each pooling layer are set uniformly to avoid information loss. Finally, the classification layer is connected to the extracted signatures with the class of the target. The settings of the classification layer are relatively fixed and have little impact on the model.

4.2. Proposed dual-frequency scale CNN

As mentioned above, the detection effect of cyber spoofing mainly depends on the defects of the convolutional layer. To eliminate this defect, the dual-frequency scale CNN with the Octave Convolution (OC) is proposed.

Actually, the power spectrum $E_{cwt}$is treated as the two-dimensional structure instead of obtaining information solely from the time or frequency axis in CNN. As shown in Fig. 7, the Fig. 7(b) and (c) are the higher and lower frequencies of Fig. 7(a) calculated using the 2D-FFT, respectively. For the two-dimensional structure, it can be seen that the higher frequency of the power spectrum is usually encoded with details, such as the start time and the magnitude of the spoofing. The lower frequency is encoded with global features, such as the length of the spoofing. Therefore, the spatial resolution can be further improved from dual-frequency scales, where the scale refers to the dimensions and information contained in the signatures extracted in the convolutional layer [56].

Then octave convolution can be used here to reduce the redundancy by considering the high frequency and low frequency features in the convolutional layer, which is first introduced in [57]. Here, the input of the DSCNN is denoted as $X = \{E_{cwt}\}_m$, where *m*is the number of training samples. The first step of OC is to process the X in two channels $X = \{X_H, X_L\}_m$, namely the high and low frequency signatures extraction channels. Meanwhile, these two channels are expected to communicate efficiently. Therefore, this interactive layer is represented as $X_{H-L}$and X_{L-H}. The output of each frequency channel can be given by $Y_H = \{Y_{H-H} + Y_{L-H}\}$ and $Y_L = \{Y_{L-L} + Y_{H-L}\}$, where the $H-L$denotes the high-dimensional data is converted to low-dimensional data using an average pooling layer, the $L-H$denotes the low-dimensional data is converted to high-dimensional data using upsampling operation. Finally, the merge operation will be used to fuse all the $Y_H$and Y_L.

Specifically, in the first layer of DSCNN, the X is spilt into X_H and X_L channels using the convolution. The output of the first layer can be obtained as

$$\begin{aligned} Y^l &= f(W^l * X + b^l) \\ &= f(W^l_H * X_H + b^l_H) + f(W^l_L * X^l_L + b^l_L) \\ &= Y^l_H + Y^l_L \end{aligned} \tag{3}$$

where * denotes the convolution operation, f is the activate function, the $W^l = \{W^l_H, W^l_L\}$ and $b^l = \{b^l_H, b^l_L\}$ are the weight and bias in two frequency channels at the lth layers, respectively. The dimension of the $Y^l_L$is only half of Y^l_H, thus the low and high frequency signatures can be extracted. Based on the first layer, the output of the next OC layer can be expressed as

$$Y^l = \{Y^l_{H-H} + Y^l_{L-H}\} + \{Y^l_{L-L} + Y^l_{H-L}\} \tag{4}$$

where the $Y^l_{H-H}$and Y^l_{L-L} are general convolutional layers and their output dimension will not change. Y^l_{L-H} and Y^l_{H-L} are the interactive signatures, which are used to enrich the feature space. Eventually, the output of each high and low frequency channel is

$$\begin{aligned} Y^l_H &= \{Y^l_{H-H} + Y^l_{L-H}\} \\ &= f(W^l_{H-H} * X_H + b^l_{H-H}) + f(W^l_{L-H} * X^l_L + b^l_{L-H}) \end{aligned} \tag{5}$$

and

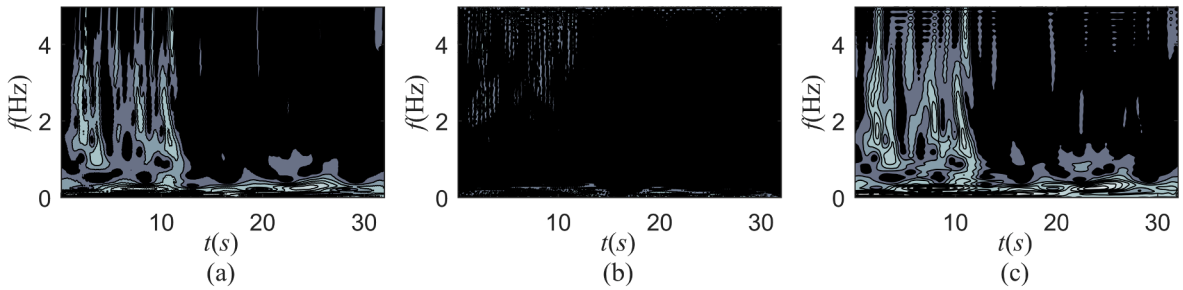

Fig. 7. The gray data of the power spectrum E_{cwt}under cyber spoofing based on 2DFFT. (a) the $E_{cwt}$of the spoofing data, (b) the higher frequency of E_{cwt}, (c) the lower frequency of E_{cwt}.

$$Y_L^l = \{Y_{L-L}^l + Y_{H-L}^l\} = f(W_{L-L}^l * X_L + b_{L-L}^l) + f(W_{H-L}^l * X_H^l + b_{H-L}^l) \quad (6)$$

Thereafter, the last step of OC in DSCNN is to add two channels together. The OC can be used to replace the regular convolution. In the low frequency channel, the data dimension is only a half of the high frequency, which not only reduces the amount of calculation, but also expands the frequency space of signatures.

Before cyber spoofing classification, a depthwise convolution is connected to the output of OC since the number of output nodes can be easily adjusted. Different from the regular convolution, the depthwise convolution needs fewer parameters while ensuring accuracy [58]. The output of a depthwise convolution is denoted as Y_d, which is flattened and then connected to the softmax function. Then, the cyber attack can be identified through the label of each input power spectrum E_{cwt}. This is a two-class classification, where the data is identified as attacked or normal.

5. Cyber security defense and identification framework

Using the proposed CWTs and DSCNN, this section further proposes a cyber spoofing defense framework CWTs-DSCNN for spoofing data detection in WAMS-based FFR control system. As shown in Fig. 8, this framework can be summarized as the following steps

- *Time-frequency based power spectrum calculation*: Performing data detrending to the synchrophasor data of the WAMS-based FFR control system using the high pass filter. Then the CWTs is applied to the filtered data to obtain the time-frequency features of the spoofing data. The time-frequency based power spectrum data are calculated as $E_{cwt}$with the shape (160, 320).
- *Cyber spoofing identification*: Establish a DSCNN model based on the extracted time-frequency based data. A total of three Octave Convolution (OC) are stacked. Based on the probability output of the softmax function, then the cyber spoofing from multiple measurement units can be identified utilizing its unique signatures. The input synchrophasor can be classified into two categories based on the output label, including the normal data and spoofing data.

As depicted in Fig. 8, the dropout is used to reduce the over-fitting. The random drop rate is empirically set to 0.5, which means that 50% of nodes are dropped during the training process. Next, the validity of CWTs-DSCNN is verified by multiple experiments.

6. Experiments

In this section, several experiments are used to verify the accuracy of the proposed method in detecting cyber spoofing attacks in the WAMS-based FFR control system. To make the attack signal closer to the real scene, the synchrophasor data collected from ten PMU units in WECC are used to simulate the cyber attack. It is more secretive if the real-time measured data of the power system is used to attack the original measurement data in the same WAMS. As shown in Fig. 9, the synchrophasor frequency data are synchronized sampling in multiple states with a 10 Hz reporting rate. Then, the data can be obtained from the FNET/GridEye sever. FNET/GridEye is a pilot wide-area phasor measurement system, which covers the national or continental level power grid [59]. The FNET/GridEye uses low-cost but high-accuracy PMU variants to achieve the power grid information collection then transmit to their data center to achieve collection and analysis [60]. Nine units are used for training and one unit is reserved for source ID tampering. The reserved unit will not participate in training and is used to simulate unknown spoofing data. The frequency data is selected to analyze the performance of CWTs-DSCNN. The collected time is in January 4-5th (training and testing), 11 −12th (the first week), 25 −26th (the third week), and April 5th (three months) of 2019.

In these experiments, both the window size and the step size are set to 320. This means that each sample contains 32s data. There are 16848 samples generated for training, and 2790 samples for verification. For the validation set, we choose one day, one week, three weeks, and three months after the training data to test the robustness of the method. Each time node has 2790 samples. For the CWTs, the Python library named PyWavelets is used, which is an open source wavelet transform software [61]. For the DSCNN, the training platform is based on GPU with GTX 1060. During the training process, an attenuated learning rate training method is used, and 30 epochs are executed in total. The Keras deep learning library is used to establish the DSCNN model.

6.1. Parameter sensitivity analysis

The parameters of DSCNN directly affect the cyber spoofing detection in WAMS-based FFR control system. To select the suitable parameters, the grid search is used to determine some main parameters, including the number of convolutional layers, kernel size, the number of nodes in the fully connected layer, and the dropout rate in the dropout layer. Both the debugging and grid search methods are used. The value range of the hyperparameters is determined through preliminary debugging. Then, the grid search is applied to select the hyperparameters. In this section, the kernel size and the number of convolutional layers are used as an example to show how to select the suitable parameters.

In this experiment, the relationship between the kernel size and the number of convolutional layers are conducted, as shown in Fig. 10. The kernel size $k$ranges from $3 \times 3$to $15 \times 15$with step size 2. The 3-layer, 4-layer, and 5-layer DSCNN denote that the number of OC layers are two, three, and four, respectively. As can be seen from Fig. 10, a larger kernel size usually has higher accuracy. Meanwhile, there is a slight drop when the k is equal to $15 \times 15$for the five-layer DSCNN. For all numbers of layers, the lowest accuracy 95.90% is obtained when the $k = 13 \times 13$. The 5-layer DSCNN reaches the highest accuracy when $k$is between $9 \times 9$and 13×13. And the 3-layer DSCNN performs better than the 4-layer

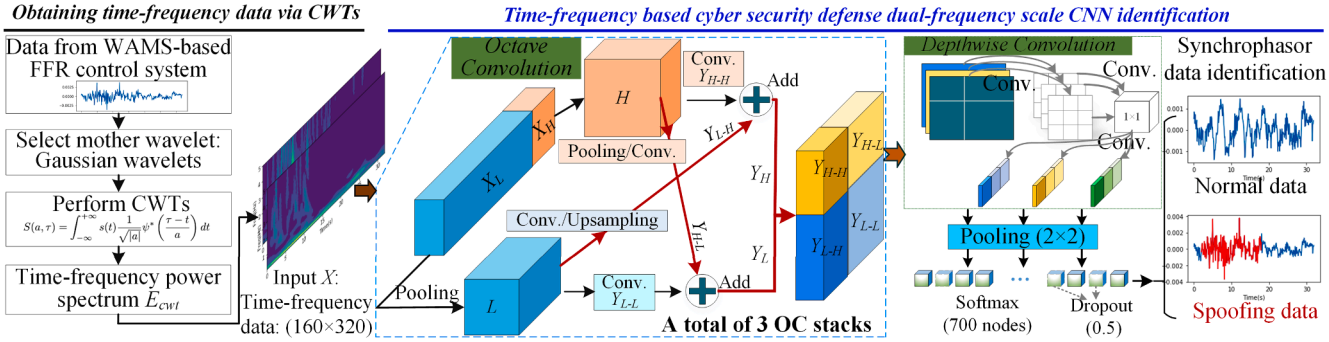

Fig. 8. The cyber spoofing defense framework based on CWTs-DSCNN. The conv. denotes the regular convolutional layer.

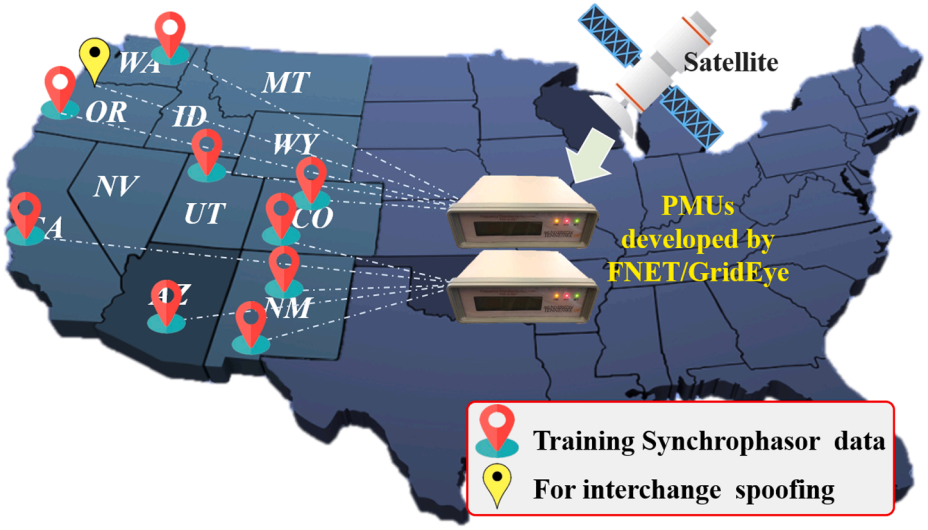

Fig. 9. The locations of ten collected frequency data in WECC system.

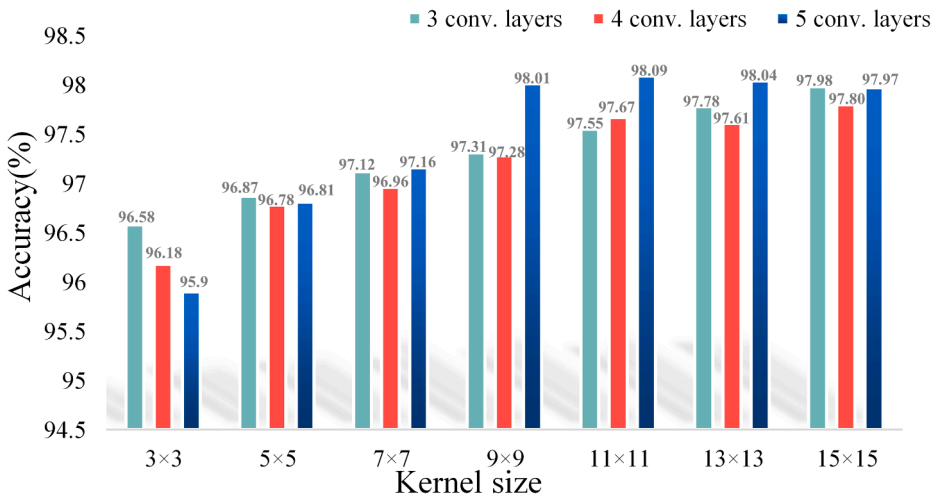

Fig. 10. The performance of DSCNN under different kernel sizes and number of convoutional layers.

for most kernel sizes. This is because that the 4-layer has fewer model parameters and therefore causes a slight decrease in accuracy. Finally, the 3-layer DSCNN is selected as a trade-off between performance and the number of model parameters.

Next, the accuracy between the kernel size and three time nodes are tested for 3-layer DSCNN, of which the result is shown in Fig. 11. The one-week time node denotes the test samples were collected one week later after collecting the training samples. It shows that the highest accuracy is located at $k = 13 \times 13$in all three time nodes. Therefore, the $k = 13 \times 13$is selected. Additionally, the test accuracy decreases with the time increase. This is reasonable because the state of the power grid is changing, including load, generation, and transmission networks. It can also be seen that the accuracy difference between one week and three weeks is about 4%, while the difference between three weeks and three months is about 13%.

6.2. *Sensitivity analysis of different test time nodes*

Generally speaking, the grid status is different between weekends and weekdays. For example, less energy demand is required on weekends [62], which leads to different time-frequency characteristics of the synchrophasor data. Based on this consideration, this paper further studies the impact of training data which collected at different time on the accuracy. Here, the 'sensitivity analysis' means the performance of the proposed method under different test time nodes. And its motivation is to explore the performance difference in different time periods. For instance, the data collected on weekdays is used for training and the data on weekends for testing. The test results are shown in Fig. 12.

From Fig. 12(a), it can be seen that the test accuracy of the weekend is higher when weekday data is used for training. The weekend data test accuracy is still very high even after three months. Similarly, when the data from the weekend is used for training, the accuracy of the weekend data test is higher, as shown in Fig. 12(b). One reason for this phenomenon is that the power grid status changes more drastically on workdays in different seasons, which leads to changes in signatures of time-frequency data. Then, when both the data of the weekends and weekdays are used for training, this difference still exists. However, the accuracy of attack detection on weekdays (78.73%) is slightly higher compared with Fig. 12(a)(76.15%) and (b)(78.09%). This implies that different time periods of synchrophasor data should be combined in training. To prevent the accuracy decrease at different times, two measures can be taken, including 1) update model parameters at regular intervals. By continuously retraining the model, the high accuracy can be maintained using the new measurement data, 2) use faster hardware and larger networks. If hardware conditions can be increased, a larger network can then be used to improve the detection effect.

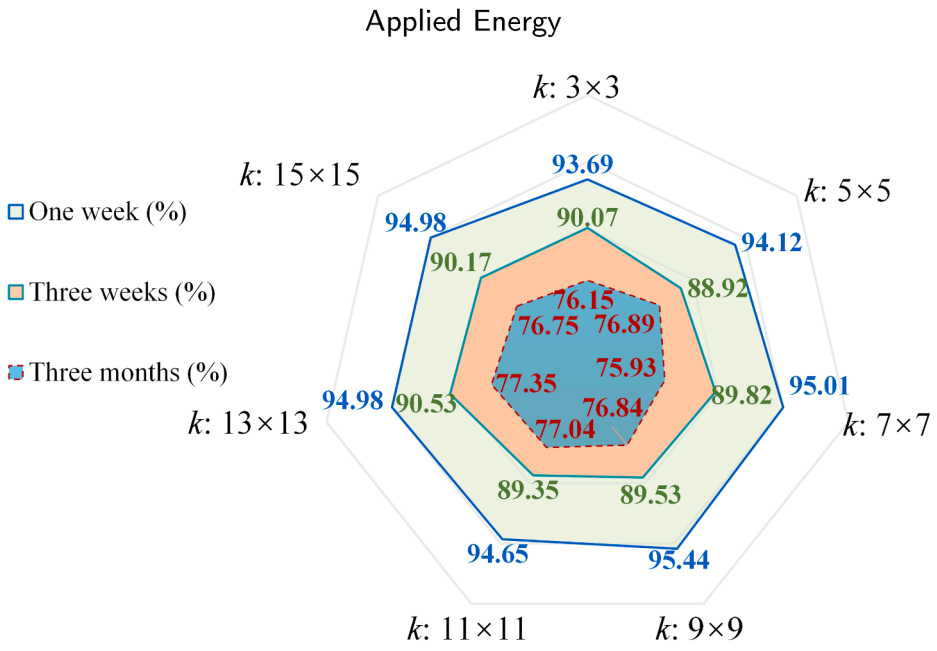

Fig. 11. Relationship between the kernel and three time nodes including one week, three weeks, and three months.

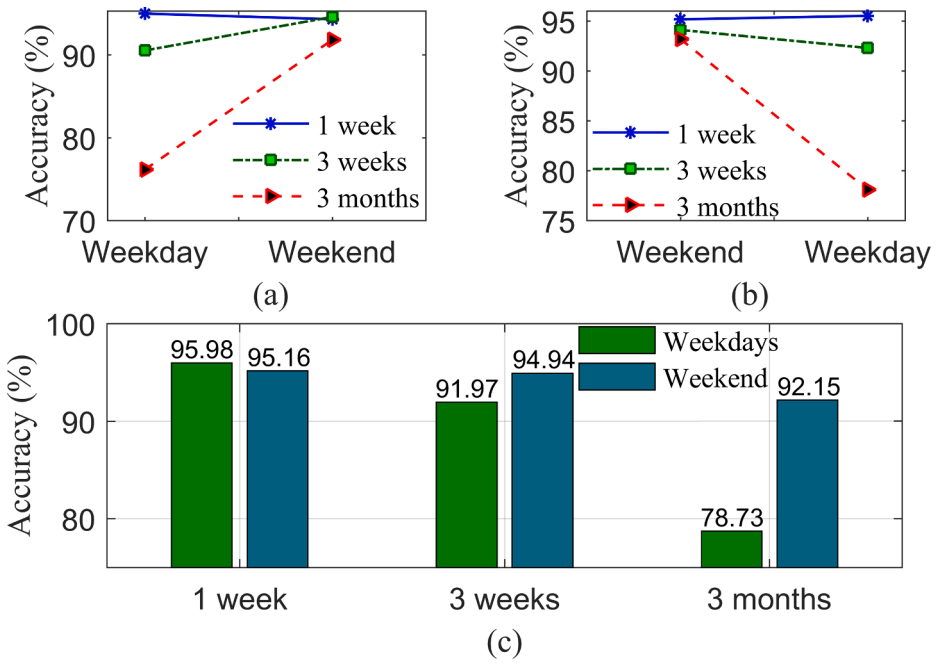

Fig. 12. The time sensitivity analysis experiment. (a) Performance when the training data is collected at weekdays, (b) performance when the training data is collected at weekdays, (c) performance when the training data is collected from both weekends and weekdays.

6.3. Identification accuracy comparison of the proposed method

Different CNN structures are designed in this section to verify the effectiveness of cyber spoofing identification. Both weekend data and weekday data are used in this section. Six methods are designed, including CWTs-Extreme Learning Machine (ELM), LSTM, FFT-One-dimensional CNN (1DCNN), CWTs-1DCNN, regular 2DCNN, and DSCNN-no depthwise convolution (De.) methods. The LSTM is a method suitable for time series processing. The two-dimensional result of CWTs is flattened and fed into a two-layer structure of ELM. The number of nodes of ELM is optimized set to 500–400. Two LSTM layers are selected and the number of nodes before the classification layer is also 700 points. The input of LSTM is the normal raw cyber spoofing frequency data. To compare the amount of information in frequency signatures, the FFT of detrended data is fed to 1DCNN. The structure of 1DCNN is referred to [63]. The motivation of CWTs-1DCNN is to verify the effectiveness of CWTs. Thus the structure of 1DCNN in CWTs-1DCNN is the same as FFT-1DCNN. For the 2DCNN, only the regular convolution is used. Meanwhile, the DSCNN without the depthwise convolution is also listed to verify its capabilities. It is worth mentioning that the number of convolutional layers is the same for 2DCNN, DSCNN-no De, and DSCNN to make a fair comparison. The identification results are listed in Table 1.

It illustrates that the result of 2DCNN is 4% higher than LSTM and

Table 1
Comparison of different detection methods.

Models	Accuracy(%)		Number of	Test time
	Oneday	Threemonths	parameter	(*ms*)
CWTs-ELM	82.07 ± 0.008	70.25	–	13.462
LSTM	92.11 ± 0.539	82.33	732 k	18.579
FFT-1DCNN	89.64 ± 0.256	78.09	72 k	0.181
CWTs-1DCNN	96.00 ± 0.490	85.16	3863 k	2.921
2DCNN	96.18 ± 0.054	84.04	596 k	3.171
DSCNN-no De.	97.35 ± 0.038	84.69	586 k	3.072
DSCNN	97.78 ± 0.012	85.44	569 k	2.480

Ave. Acc.: Average accuracy, k: thousand.

6% higher than FFT-1DCNN, indicating that the time-frequency based signatures contain more information compared with the single time or frequency domain information. The result of CWTs-ANN and CWTs-2DCNN shows that CNN has stronger feature extraction and cyber attack detection ability. Although FFT-1DCNN has fewer parameters, the uncertainty reached 0.256%, which means that the model is unstable. FFT-1DCNN can also be used for the big data analysis scenario considering its fast calculation performance. The performance of FFT-1DCNN and CWTs-1DCNN shows that the CWTs contribute to accuracy improvement. The DSCNN-no De. obtains 1.2% and 0.65% higher accuracy in one-day and three-month testing, respectively. And the DSCNN outperforms the 2DCNN and DSCNN-no De. in the one-day and three-month testing, indicating that the proposed method has profound reliability. Meanwhile, the number of parameters is smaller and the running time of DSCNN is also less. This means that both the octave and depthwise convolution are beneficial to the efficiency of cyber spoofing identification.

6.4. Performance comparison with advanced methods

The last experiment is to compare the performance of CWTs-DSCNN with some advanced cyber spoofing detection methods, including FFT-ANN [43], MM-RFC [41], MM-gcForest [40], and EEMD-FFT-BP [42]. For FFT-ANN and EEMD-FFT-BP, only the frequency domain information (amplitude spectrum) is used for cyber spoofing detection. In MM-RFC and MM-gcForest, more than 60 statistical features are extracted. The CWTs-ANN is used to verify the effectiveness of CWTs, where the ANN is the same structure as FFT-ANN. The F1 score is used and can be interpreted as a weighted average of the precision and recall, where a value closer to 1 indicates a better model [64]. The performance under different time nodes are tested, as listed in Table 2. The test time consists of signature extraction and spoofing identification for 2790 samples.

As can be seen from Table 2, FFT-ANN has better accuracy and stability compared with EEMD-FFT-BP because an accuracy higher than 83% is obtained for both one week and three weeks time nodes. It also has minimal time consumption, because multiple decompositions need to be calculated in EEMD. As for the FFT-ANN, MM-RFC, and MM-gcForest, the MM-gcForest obtains better accuracy even after three months. In terms of time consumption, the MM-gcForest is suitable for occasions with fast calculation and long-term operational requirements. The FFT-ANN has better performance in one week and it is suitable for short-term operation and small sample learning scenarios. The MM-RFC obtains the lowest accuracy since it has the lower F1 score and accuracy than the rest of the models. Thus it is recommended to use MM-gcForest when facing the same fast demand. And the CWTs-DSCNN has profound performance in all three time nodes. This means that the CWTs contributes to spoofing data recognition. Compared with the FFT-ANN and CWTs-ANN, it shows that the CWTs-ANN obtains higher accuracy after three months because more information is extracted in CWTs.

Moreover, it can be seen that 85.44% accuracy is reached even after three months for CWTs-DSCNN. The test time is about 268s due to the calculation of CWTs. Real-time performance can also be satisfied because each sample (320 points means 32s) only consumes 96 ms. Based on the above analysis, the proposed CWTs-DSCNN has a superior performance because it has high-quality input information and a high-precision classifier.

Table 2
Performance comparison with advanced methods

Models	Accuracy (%)			Test time/s	F1 score
	1week	3weeks	3months		(one day)
FFT-ANN [43]	85.32	83.45	72.60	**0.297**	0.887
CWTs-ANN	86.31	82.25	79.56	261.708	0.890
MM-RFC [41]	74.40	70.15	68.08	5.047	0.737
MM-gcForest [40]	82.15	78.85	75.95	5.488	0.823
EEMD-FFT-BP [42]	73.51	71.58	60.10	2301.526	0.846
CWTs-DSCNN	**95.57**	**93.45**	**85.44**	268.369	**0.979**

7. Conclusion

To enhance the stable operation of the WAMS-based FFR control system under various cyber attacks, in this paper, a time-frequency based cyber security defense framework called CWTs-DSCNN is proposed to detect the cyber spoofing of synchrophasor data in the WAMS-based FFR control system. In the defense framework, the time-frequency matrix is first transformed using CWTs. The normal and spoofing time-frequency information of CWTs shows that unique signatures can be extracted efficiently. Then, DSCNN is proposed to identify the time-frequency based power spectrum based on the dual-frequency scale. Utilizing the data from FNET/GridEye, appropriate parameters of DSCNN are selected through parameter analysis experiments. The comparison with some advanced and commonly used methods reveals that the proposed method has a stronger detection capability for cyber spoofing attacks. In addition, the detection time and the amount of parameters are also reduced by using DSCNN, which makes it appropriate to be applied in the WAMS-based FFR control system. Time sensitivity analysis experiments evidence that the data of different time nodes need to be combined to fully describe the signature of synchrophasor data.

There are several promising directions for future research. One topic could focus on the real-time calculation, which could be achieved by reducing the amount of calculation of CWTs. Another interesting topic is the complete detecting and response framework, which could realize the fast attack detection and provide effective response strategy to mitigate the cyber attack influence as soon as possible.

CRediT authorship contribution statement

Wei Qiu: Conceptualization, Data curation, Methodology, writing - original draft. **Kaiqi Sun:** Conceptualization, Methodology, Visualization, writing - original draft. **Wenxuan Yao:** Formal analysis, Investigation, Resources. **Shutang You:** Writing – review & editing, Formal analysis. **He Yin:** Data curation, Formal analysis, writing – review & editing. **Xiaoyang Ma:** Writing – review & editing, Visualization. **Yilu Liu:** Writing – review & editing, Supervision.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This work was also supported by the NSF Cyber-Physical Systems (CPS) Program (#1931975).

References

[1] Lv T, Ai Q. Interactive energy management of networked microgrids-based active distribution system considering large-scale integration of renewable energy resources. Appl Energy 2016;163:408–22. https://doi.org/10.1016/j.apenergy.2015.10.179.

[2] Sun K, Li KJ, Pan J, Liu Y, Liu Y. An optimal combined operation scheme for pumped storage and hybrid wind-photovoltaic complementary power generation system. Appl Energy 2019;242:1155–63. https://doi.org/10.1016/j.apenergy.2019.03.171.

[3] REN21. Renewables 2020 global status report. Rep. Paris: REN20; 2020.

[4] IRENA, Untapped potential for climate action: renewable energy in nationally determined contributions https://www.irena.org/publications/2017/Nov/Untapped-potential-for-climate-action-NDC.

[5] Gomis-Bellmunt O, Junyent-Ferré A, Sumper A, Galceran-Arellano S. Maximum generation power evaluation of variable frequency offshore wind farms when connected to a single power converter. Appl Energy 2010;87:3103–9. https://doi.org/10.1016/j.apenergy.2010.04.025.

[6] Zhu J, Booth CD, Adam GP, Roscoe AJ, Bright CG. Inertia emulation control strategy for vsc-hvdc transmission systems. IEEE Trans Power Syst 2013;28:1277–87.

[7] Tielens P, Van Hertem D. The relevance of inertia in power systems. Renew Sustain Energy Rev 2016;55:999–1009. https://doi.org/10.1016/j.rser.2015.11.016.

[8] Zhu X, Xia M, Chiang HD. Coordinated sectional droop charging control for ev aggregator enhancing frequency stability of microgrid with high penetration of renewable energy sources. Appl Energy 2018;210:936–43. https://doi.org/10.1016/j.apenergy.2017.07.087.

[9] Cheng Y, Azizipanah-Abarghooee R, Azizi S, Ding L, Terzija V. Smart frequency control in low inertia energy systems based on frequency response techniques: A review. Appl Energy 2020;279:115798. https://doi.org/10.1016/j.apenergy.2020.115798.

[10] Sun K, Xiao H, Liu S, You S, Yang F, Dong Y, et al. A review of clean electricity policies–from countries to utilities. Sustainability 2020;12:7946.

[11] Kim Y, Del-Rosario-Calaf G, Norford LK. Analysis and experimental implementation of grid frequency regulation using behind-the-meter batteries compensating for fast load demand variations. IEEE Trans Power Syst 2017;32:484–98.

[12] Karbouj H, Rather ZH, Flynn D, Qazi HW. Nonsynchronous fast frequency reserves in renewable energy integrated power systems A critical review. Int J Electr Power Energy Syst 2019;106:488–501. https://doi.org/10.1016/j.ijepes.2018.09.046.

[13] NERC. Fast frequency response concepts and bulk power system reliability needs; 2020. https://www.nrel.gov/grid/ieee-standard-1547/bulk-power-reliability-needs.html.

[14] You S, Liu Y, Liu Y, Till A, Li H, Su Y, et al. Energy storage for frequency control in high photovoltaic power grids, in. In: IEEE EUROCON 2019–18th International Conference on Smart Technologies; 2019. p. 1–6.

[15] CAISO. Frequency response phase 2 issue paper; 2016. https://www.caiso.com/Documents/IssuePaper_FrequencyResponsePhase2.pdf.

[16] McGill R, Torres-Olguin R, Anaya-Lara O, Leithead W. Generator response following as a primary frequency response control strategy for VSCHVDC connected offshore wind farms. Energy Procedia 2017;137:108–18. https://doi.org/10.1016/j.egypro.2017.10.338. 14th Deep Sea Offshore Wind R&D Conference, EERA DeepWind'2017.

[17] Neely J, Johnson J, Delhotal J, Gonzalez S, Lave M. Evaluation of pv frequency-watt function for fast frequency reserves. In: 2016 IEEE Applied Power Electronics Conference and Exposition (APEC); 2016. p. 1926–33.

[18] Peltonen L, Järventausta P, Repo S, Rauhala T. Distributed small loads as fast frequency reserves: Impact on system performance, in. In: 2020 IEEE Texas Power and Energy Conference (TPEC); 2020. p. 1–6.

[19] Sun K, Xiao H, You S. Frequency secure control strategy for power grid with largescale wind farms through hvdc links. Int J Electr Power Energy Syst 2020;117:105706. https://doi.org/10.1016/j.ijepes.2019.105706.

[20] Junyent-Ferr A, Pipelzadeh Y, Green TC. Blending hvdc-link energy storage and offshore wind turbine inertia for fast frequency response. IEEE Trans Sustain Energy 2015;6:1059–66.

[21] Adeuyi OD, Cheah-Mane M, Liang J, Jenkins N. Fast frequency response from offshore multiterminal vsc–hvdc schemes. IEEE Trans Power Deliv 2017;32:2442–52.

[22] Vrettos E, Ziras C, Andersson G. Fast and reliable primary frequency reserves from refrigerators with decentralized stochastic control. IEEE Trans Power Syst 2017;32:2924–41.

[23] Chakravorty D, Chaudhuri B, Hui SYR. Rapid frequency response from smart loads in great britain power system. IEEE Trans Smart Grid 2017;8:2160–9.

[24] Craciun B, Kerekes T, Séra D, Teodorescu R. Frequency support functions in large pv power plants with active power reserves. IEEE J Emerg Sel Top Power Electron 2014;2:849–58.

[25] You S, Liu Y, Kou G, Zhang X, Yao W, Su Y, et al. Non-invasive identification of inertia distribution change in high renewable systems using distribution level pmu. IEEE Trans Power Syst 2018;33:1110–2.

[26] Liu Y, You S, Liu Y. Study of wind and pv frequency control in u.s. power grids–ei and ti case studies. IEEE Power Energy Technol Syst J 2017;4:65–73.

[27] Hong Q, Karimi M, Sun M, Norris S, Bagleybter O, Wilson D, et al. Design and validation of a wide area monitoring and control system for fast frequency response. IEEE Trans Smart Grid 2020;11:3394–404.

[28] Wang W, Sun K, Zeng C, Chen C, Qiu W, You S, et al. Information and Communication Infrastructures in Modern Wide-Area Systems. Cham: Springer International Publishing; 2021. p. 71–104.

[29] Sahoo S, Peng JC, Mishra S, Dragicevic T. Distributed screening of hijacking attacks in dc microgrids. IEEE Trans Power Electron 2020;35:7574–82.

[30] Pan K, Rakhshani E, Palensky P. False data injection attacks on hybrid ac/hvdc interconnected systems with virtual inertia–vulnerability, impact and detection. IEEE Access 2020;8:141932–45.

[31] Gelenbe E, Kadioglu YM. Energy life-time of wireless nodes with network attacks and mitigation. In: 2018 IEEE International Conference on Communications Workshops (ICC Workshops); 2018. p. 1–6.

[32] Zhao P, Gu C, Huo D. Coordinated risk mitigation strategy for integrated energy systems under cyber-attacks. IEEE Trans Power Syst 2020;35:4014–25.

[33] Ameli A, Hooshyar A, Yazdavar AH, El-Saadany EF, Youssef A. Attack detection for load frequency control systems using stochastic unknown input estimators. IEEE Trans Inf Forensics Secur 2018;13:2575–90. https://doi.org/10.1109/TIFS.2018.2824253.

[34] Chen C, Zhang K, Yuan K, Zhu L, Qian M. Novel detection scheme design considering cyber attacks on load frequency control. IEEE Trans Industr Inf 2018;14:1932–41. https://doi.org/10.1109/TII.2017.2765313.

[35] Chen C, Zhang K, Ni M, Wang Y. Cyber-attack-tolerant frequency control of power systems. J Modern Power Syst Clean Energy 2020;1–9. https://doi.org/10.35833/MPCE.2019.000185.

[36] Aluko AO, Carpanen RP, Dorrell DG, Ojo EE. Impact assessment and mitigation of cyber attacks on frequency stability of isolated microgrid using virtual inertia control. In: 2020 IEEE PES/IAS PowerAfrica; 2020. p. 1–5. doi: 10.1109/PowerAfrica49420.2020.9219790.

[37] Keshtkar H, Mohammadi FD, Ghorbani J, Solanki J, Feliachi A. Proposing an improved optimal lqr controller for frequency regulation of a smart microgrid in case of cyber intrusions. In: 2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE); 2014. p. 1–6.

[38] Deng R, Zhuang P, Liang H. False data injection attacks against state estimation in power distribution systems. IEEE Trans Smart Grid 2019;10:2871–81.

[39] Musleh AS, Chen G, Dong ZY. A survey on the detection algorithms for false data injection attacks in smart grids. IEEE Trans Smart Grid 2020;11:2218–34. https://doi.org/10.1109/TSG.2019.2949998.

[40] Cui Y, Bai F, Liu Y, Fuhr PL, Morales-Rodríguez ME. Spatio-temporal characterization of synchrophasor data against spoofing attacks in smart grids. IEEE Trans Smart Grid 2019;10:5807–18.

[41] Cui Y, Bai F, Liu Y, Liu Y. A measurement source authentication methodology for power system cyber security enhancement. IEEE Trans Smart Grid 2018;9:3914–6.

[42] Liu S, You S, Yin H, Lin Z, Liu Y, Yao W, et al. Model-free data authentication for cyber security in power systems. IEEE Trans Smart Grid 2020;11:4565–8.

[43] Yao W, Zhao J, Till MJ, You S, Liu Y, Cui Y, et al. Source location identification of distribution-level electric network frequency signals at multiple geographic scales. IEEE Access 2017;5:11166–75.

[44] Landford J, Meier R, Barella R, Wallace S, Zhao X, Cotilla-Sanchez E, et al. Fast sequence component analysis for attack detection in smart grid. In: 2016 5th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS); 2016. p. 1–8.

[45] Khalid HM, Peng JC. Immunity toward data-injection attacks using multisensor track fusion-based model prediction. IEEE Trans Smart Grid 2017;8:697–707. https://doi.org/10.1109/TSG.2015.2487280.

[46] Wang J, Shi D, Li Y, Chen J, Ding H, Duan X. Distributed framework for detecting pmu data manipulation attacks with deep autoencoders. IEEE Trans Smart Grid 2019;10:4401–10.

[47] Habibi MR, et al. Detection of false data injection cyber-attacks in dc microgrids based on recurrent neural networks. IEEE J Emerg Sel Top Power Electron 2020:1.

[48] Pei J, Wang J, Shi D. Data-driven measurement tampering detection considering spatial-temporal correlations. In: 2019 IEEE 3rd Conference on Energy Internet and Energy System Integration (EI2); 2019. p. 2641–6.

[49] PE/PSCC/- Power System Communications and Cybersecurity. IEEE Standard for Synchrophasor Data Transfer for Power Systems. IEEE Std C37.118.2-2011 (Revision of IEEE Std C37.118-2005); 2011. p. 1–53.

[50] Tu C, He X, Liu X, Li P. Cyber-Attacks in PMU-Based Power Network and Countermeasures. IEEE Access 2018;6:65594–603.

[51] Toppa S. Available: https://bit.ly/1FH246I. The National Power Grid Is Under Almost Continuous Attack, Report Says, Time.com.

[52] Cui Y, Wang W, Liu Y, Fuhr P, Morales-Rodriguez M. Spatio-temporal synchrophasor data characterization for mitigating false data injection in smart grids. In: 2019 IEEE Power Energy Society General Meeting (PESGM); 2019. p. 1–5.

[53] Cnockaert L, Migeotte P, Daubigny L, Prisk GK, Grenez F, Sa RC. A method for the analysis of respiratory sinus arrhythmia using continuous wavelet transforms. IEEE Trans Biomed Eng 2008;55:1640–2.

[54] Qiu W, et al. An automatic identification framework for complex power quality disturbances based on multifusion convolutional neural network. IEEE Trans Industr Inf 2020;16:3233–41. https://doi.org/10.1109/TII.2019.2920689.

[55] Qiu W, Tang Q, Liu J, Teng Z, Yao W. Power Quality Disturbances Recognition Using Modified S Transform and Parallel Stack Sparse Auto-encoder. Electr Power Syst Res 2019;174:105876.

[56] Lindeberg T. Scale-Space Theory in Computer Vision; 1993. http://www.nada.kth.se/tony/book.html. qC20110913.

[57] Chen Y, Fan H, Xu B, Yan Z, Kalantidis Y, Rohrbach M, et al. Drop an octave: Reducing spatial redundancy in convolutional neural networks with octave convolution. In: 2019 IEEE/CVF International Conference on Computer Vision (ICCV); 2019. p. 3434–43.

[58] Borwankar R, Ludwig R. A novel compact convolutional neural network for real-time nondestructive evaluation of metallic surfaces. IEEE Trans Instrum Meas 2020;69:8466–73.
[59] Liu Y, You S, Yao W, Cui Y, Wu L, Zhou D, et al. A distribution level wide area monitoring system for the electric power grid–fnet/grideye. IEEE Access 2017;5:2329–38. https://doi.org/10.1109/ACCESS.2017.2666541.
[60] Wang W, Sun K, Chen C, Wei Q, He Y, You S, et al. Advanced synchrophasor-based application for potential distributed energy resources management: Key technology, challenge and vision. In: 2020 IEEE/IAS Industrial and Commercial Power System Asia (I CPS Asia); 2020. p. 1120–4. doi:10.1109/ICPSAsia48933.2020.9208606.
[61] Lee GR, et al. PyWavelets A Python package for wavelet analysis. J Open Source Softw 2019;4:1237. https://doi.org/10.21105/joss.01237.
[62] Carmon D, Navon A, Machlev R, Belikov J, Levron Y. Readiness of small energy markets and electric power grids to global health crises: Lessons from the covid-19 pandemic. IEEE Access 2020;8:127234–43.
[63] Wang S, Chen H. A novel deep learning method for the classification of power quality disturbances using deep convolutional neural network. Appl Energy 2019;235:1126–40. https://doi.org/10.1016/j.apenergy.2018.09.160. http://www.sciencedirect.com/science/article/pii/S0306261918314703.
[64] Derczynski L. Complementarity, Fscore, and NLP Evaluation. In: Proceedings of the Tenth International Conference on Language Resources and Evaluation (LREC'16), European Language Resources Association (ELRA); 2016. p. 261–6.