# Multi-View Convolutional Neural Network for Data Spoofing Cyber-Attack Detection in Distribution Synchrophasors

Wei Qiu, Qiu Tang, Yajun Wang, *Member, IEEE*, Lingwei Zhan, *Member, IEEE*, Yilu Liu, *Fellow, IEEE*, and Wenxuan Yao, *Member, IEEE*

***Abstract*—Security of Distribution Synchrophasors Data (DSD) is of paramount importance as the data is used for critical smart grid applications including situational awareness, advanced protection, and dynamic control. Unfortunately, the DSD are attractive targets for malicious attackers aiming to damage grid. Data spoofing is a new class of deceiving attack, where the DSD of one Phasor Measurement Units (PMUs) is tampered by other PMUs thereby spoiling measurement based applications. To address this issue, a source authentication based data spoofing attack detection method is proposed using Multi-view Convolutional Neural Network (MCNN). First, common components embedded in raw frequency measurements from DSD are removed by Savitzky-Golay (SG) filter. Second, fast S transform (FST) is utilized to extract representative spatial fingerprints via time frequency analysis. Third, the spatial fingerprint is fed to MCNN, which combines dilated and standard convolutions for automatic feather extraction and source identification. Finally, according to the output of MCNN, spoofing attack detection is performed via threshold criterion. Extensive experiments with actual DSD from multiple locations in FNET/Grideye are conducted to verify the effectiveness of the proposed method.**

***Index Terms*—Data spoofing attack, distribution synchrophasors data, multi-view convolutional neural network, source authentication.**

## Nomenclature

### *Acronyms*

| | |
|---|---|
| CI | Confidence Index |
| CNN | Convolutional neural networks |
| DSD | Distribution Synchrophasors Data |
| FST | Fast S transform |
| LSP | Least-squares polynomial |
| MCNN | Multi-view convolutional neural network |
| PMUs | Phasor Measurement Unit |
| SG | Savitzky-Golay |
| t-SNE | t-Distributed Stochastic Neighbor Embedding. |

### *Sets*

| | |
|---|---|
| $L_a$ | Length of the spoofed data |
| $L_w$ | Length of the sample |
| $M$ | Length of local symmetry data window in SG |
| $Q$ | Number of DSD classes. |

### *Functions*

| | |
|---|---|
| $C_i$ | Output of the convolution layer |
| $C_i^{\gamma}$ | Output of dilated convolutional layer |
| $C_{\gamma i}$ | Combined output of dilated and standard convolution |
| $F_i$ | Output of full connected layer |
| $P_i$ | Output of max pooling layer |
| $S(F)$ | Output probability value of softmax. |

### *Variables*

| | |
|---|---|
| $A(m, h)$ | Magnitude of FST |
| $A_a$ | Average accuracy for spoofed data |
| $b_i$ | Bias term of convolution layer |
| $d_c$ | Depth of convolution kernel |
| $f_c$ | Size of convolution kernel |
| $f_p$ | Size of pooling layer |
| $h$ | Length of the matrix $A(m, h)$ |
| $l(n)$ | Common data components |
| $m$ | Width of the matrix $A(m, h)$ |
| $M_r$ | Misidentification rate of non-spoofed data |
| $N_a$ | Non-spoofed data accuracy |
| $p$ | Order of a LSP |
| $r$ | Gaussian window parameter |
| $s_c$ | Stride of convolution kernel |
| $t(n)$ | Filtered frequency components |
| $T_{s(f)}$ | Threshold of softmax classifier |
| $t_w(n)$ | Target signal of $t(n)$ |
| $w_i$ | Weight of the convolutional kernel |

Manuscript received April 2, 2019; revised July 27, 2019 and December 3, 2019; accepted January 19, 2020. Date of publication February 3, 2020; date of current version June 19, 2020. This work was supported in part by the Engineering Research Center Program of the National Science Foundation and the Department of Energy under NSF Award EEC-1041877, and in part by the CURENT Industry Partnership Program. Paper no. TSG-00499-2019. *(Corresponding author: Wenxuan Yao.)*

Wei Qiu and Qiu Tang are with the College of Electrical and Information Engineering, Hunan University, Changsha 410082, China (e-mail: qiuwei@hnu.edu.cn; tangqiu@hnu.edu.cn).

Yajun Wang is with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996 USA (e-mail: ywang139@vols.utk.edu).

Lingwei Zhan is with the Electrical and Electronics Systems Research Division, Oak Ridge National Laboratory, Oak Ridge, TN 37830 USA (e-mail: zhanl@ornl.gov).

Yilu Liu and Wenxuan Yao are with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996 USA, and also with the Electrical and Electronics Systems Research Division, Oak Ridge National Laboratory, Oak Ridge, TN 37830 USA (e-mail: liu@utk.edu; wyao3@vols.utk.edu).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2020.2971148

| | |
|---|---|
| $x(n)$ | Frequency measurements of DSD |
| $\gamma$ | Dilated factor of dilated convolution |
| $\lambda$ | Proportion of data spoofing |
| $\rho$ | Parameter of dropout. |

## I. Introduction

SINCE electric power grids' dependence on information provided by Distribution Synchrophasor Data (DSD) is increasing, the cyber security concerns of synchrophasor communication network must be carefully addressed [1]-[3]. Some potential attacks have already been recognized, including Communication Link Damage (CLD), Denial of Service (DoS), and data spoofing [4]. CLD can be caused by physical attacks like cut-off or natural disasters, e.g., hurricanes or wild fires [5]. DoS attacks occur when a number of computers or network services in the intranet are controlled by trojans and huge redundant data traffic or inquiries to the target are generated in order to saturate the communication link [6]. As both CLD and DoS may result in significant communication delay or even missing data, existing technologies can detect these attacks with no difficulty.

Comparatively, data spoofing occurs when the Phasor Measurement Units (PMUs) are hacked by adversaries, who can arbitrarily manipulate the synchrophasors data. The data spoofing attacks can be seen as a specific implementation of data injection attacks, including various attack methods [7]. For example, data tampering and replay attacks can be easily detected by continuously monitoring the correlation coefficients between the afflicted PMUs [8].

However, if malicious intruders are familiar with the synchrophasors network configuration, data spoofing attacks may be performed and avoided the detections of existing approaches. For example, attackers can tamper or mix the measurement data of one DSD from other DSDs in different locations without major change of measurement values. Compared to random spoofing, it makes the attack much harder to be distinguished when original data is tampered by data in other location because the spoofed data have high similarity with normal data [25]. As a result, the source authentication can no longer be trusted, resulting in the estimated disturbance localization being affected. Even worse, measurement based applications are adversely influenced such as faulty result of state estimator and failure of wide area damping control since the tampered measurement still appear to be normal data [9]. Additionally, the PMU spoofing can happen in data servers such as Phasor Data Concentrators (PDC) or during data communication by malicious attacker because the IEEE C37.118.2 protocol does not offer confidentiality [10]. As an increasing number of DSD deployed in power grids, the necessity to detect such data spoofing attack and enhance cyber security of synchrophasor network arises.

Data spoofing and intrusion detection method is considered as a defense-in-depth method by the National Institute of Standards and Technology [11]. Generally, such methods are classified into two types: the anomaly detection and signature-based detection [12]. The anomaly detection method seeks the degree of deviation between observed data to determine data spoofing attacks. For example, the Local Outlier Factor (LOF), a density-based method, is used to detect falsified data in synchrophasor voltage and current curves [13]. However, the density and shape features of the replay attack are similar, thus making it difficult to identify by LOF. An ensemble-based method is used to improve the accuracy of multiple attack scenarios [14]. As described in [15], three kinds of anomaly detection methods are concentrated to comprehensively identify anomalies in the synchrophasor voltage. However, the anomaly detection methods based on density or distance are easily circumvented by adjusting data spoofing behavior, such as adjusting the length and magnitude of spoofed data.

The objective of this paper is to develop a source authentication method using spatial anomaly-based for data spoofing cyber-attack detection. It is demonstrated in [16] that the synchronized frequency measurement from DSD has its own and unique spatial fingerprint from its local grid, which is mainly determined by the topology of distribution network. Thus, these distinct spatial fingerprints, if successfully extracted, can be potential used as fingerprints for source authentication. When a data spoof attack occurs, the original spatial fingerprint embedded in the DSD from one location will be missing or replaced by fingerprints in other locations, partial or wholly [17]. Consequently, the integrity of spatial fingerprint can provide a supportive evidence for the detection of spoofing attack.

The remainder of this paper is organized as follows. Section II introduces the work related to the anomaly-based detection method. Then the framework of the proposed method is presented in Section III. Section IV introduces the principle of DSD spoofing detection method. In Section V, the feature visualization is presented to demonstrate the effectiveness of MCNN. Then, the experiments with actual DSD are conducted in Section VI. Finally, the conclusion and discussion are presented in Section VII.

## II. Related Work

The anomaly-based method first extracts valid spatial fingerprint information and then recognizes it by the classifier. The premise to identify the source of an unknown DSD from frequency measurements is to extract its characteristic since the frequency measured within a same interconnection share the same main trend due to the synchronicity of AC power system. Additionally, the common components in DSD is stochastic since it is determined by generation and load in power system. Thus the first step is to remove the common component and extract the spatial fingerprint. In [16], a Daubechies Wavelet Transform (WT) is used to decompose the original frequency measurements into high and low components. However, the selection of wavelet basis directly affects the filtering effect. A weighted high pass filter is applied on DSD for variation extrication in [18]. However, different weight vectors introduce computational errors and time delay on the original data. In this paper, we use the high-efficiency Savitzky-Golay (SG) filter [19] to eliminate common components and preserve the key spatial information without time delay.

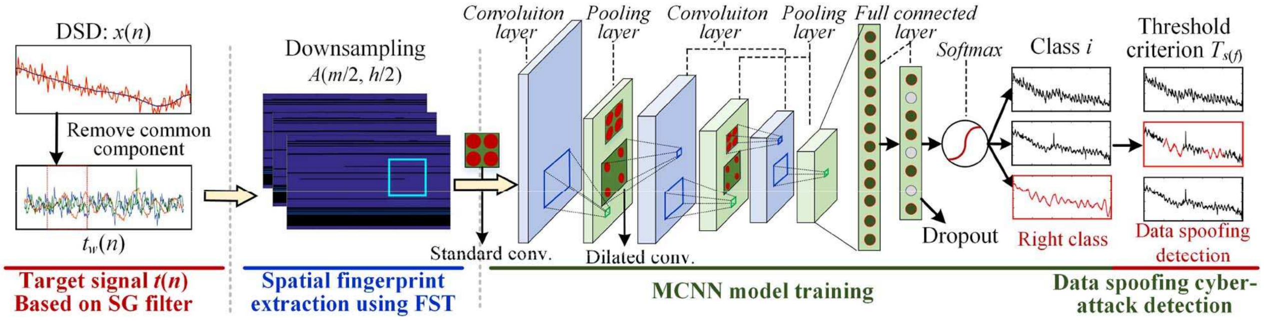

Fig. 1. The proposed framework for DSD spoofing attack detection based on MCNN.

To extract spatial information of DSD, the signal processing methods are required. Generally, the Hilbert Huang Transform (HHT) [20] and Variational Mode Decomposition (VMD) [21] are widely used for signal decomposition at time and frequency scales. The number of intrinsic mode function is empirically selected for different power signals in HHT and VMD. However, the spoofed signal is complicated due to different spoofing level. Then Empirical Orthogonal Functions (EOF) analysis is proposed to extract frequency wave components in [22], but the EOF features of statistical model are ambiguous and does not contain frequency information. Furthermore, the S-transform (ST) with the ability to provide both the time and frequency domain information is a preferred technique in signal decomposition [23]. It can detect frequency domain characteristics of the input signal in different time periods. Moreover, the computation complexity of ST can be significantly reduced via its fast implementation [24]. Therefore, the Fast ST (FST) is utilized to extract spatial fingerprints of filtered DSD at multiple frequency scales.

For the purpose of source location identification and data spoofing attack detection in DSD, a classifier is needed, which can be established by training with historical spatial fingerprints. In [25] and [26], the statistical features, including roughness index, sparsity trends, and correlation deviation, are designed to process source authentication. Then the machine learning methods, e.g., Sparse Logistic Regression and Support Vector Machines (SVM) [27], [28], are used for attack detection based on extracted features. However, for different attack levels, such as different ratio between of spoofed and normal data, a limited number of handcrafted features are difficult to represent the characteristics of different cyber-attacks data. Therefore, these detection methods using handcrafted features are not suitable for detecting diverse cyber-attack.

With the rise of deep learning algorithms, the development of Convolutional Neural Networks (CNN) has provided new ideas for grid data processing [29]. The CNN can learn effective information through supervised learning method due to the development of convolution operations, pooling layers, and computer technology. It is demonstrated that the CNN can automatically extract a large number of invariant and discriminative features for two-dimensional data [30]. In [32], the WT and CNN are combined to provide solutions for voltage signal identification. However, the standard convolution operation limits the variety of features especially for unknown data [32].

In this work, we propose a cyber-attack detection framework based on SG, FST and Multi-view Convolutional Neural Network (MCNN), where are first used in cyber-attack detection. Particularly, a MCNN with dilated convolution is presented to automatically extract features from a number of different receptive area. On top of that, MCNN can provide an attack Confidence Index (CI) based on matching level between extracted spatial fingerprints from testing data and the trained neural network. Finally, the threshold decision is made based on the proposed CI threshold criterion, where it is considered that an attack behavior has occurred when the classification output of MCNN is less than the threshold.

## III. Framework for the DSD Spoofing Detection

The framework of the proposed method for DSD spoofing detection is shown in Fig. 1. The automatic detection process can be mainly divided into four steps:

1) Signal filtering: The frequency trend of the DSD $x(n)$ is captured via Savitzky-Golay filter. Then the common frequency components are eliminated from the raw data and the target signal $t_w(n)$ is obtained.
2) Spatial fingerprint extraction: Spatial fingerprints of DSD are extracted using FST. Then the magnitude matrix $A(m/2, h/2)$ of FST is fed to the MCNN classifier.
3) MCNN model training: A multilayer MCNN model is designed and trained using extracted spatial fingerprint from historical ambient DSD without being spoofed.
4) Data spoofing cyber-attack detection: The trained MCNN model is used to authenticate incoming DSD for spoofing cyber-attack detection using threshold $T_{s(f)}$.

## IV. Principle of the DSD Spoofing Detection

### A. Savitzky-Golay Filtering

Since measurements in same interconnection have high similarity due to the synchronicity of AC power system and only spatial fingerprints from local power grid are of interest, it is essential to remove the common components for each DSD to extract the representative components. To this end, Savitzky-Golay filter is utilized to eliminate the common components and extract the local variations. Compared with common filtering algorithms, e.g., mean filtering and Kalman filtering [33],

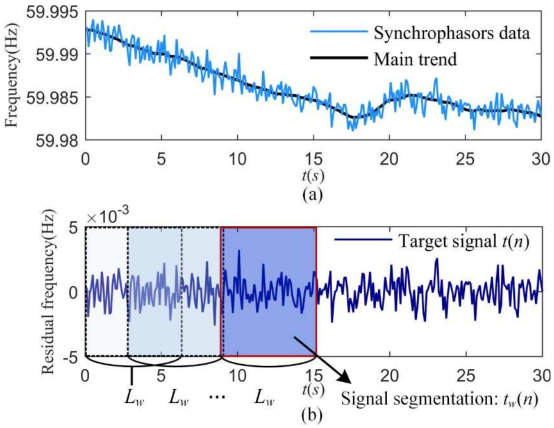

Fig. 2. Illustration of SG filtering effect on raw DSD. (a) Plot of raw frequency and captured main trend with $p = 3$ and $M = 70$, (b) Plot of target signal $t(n) = x(n) - l(n)$.

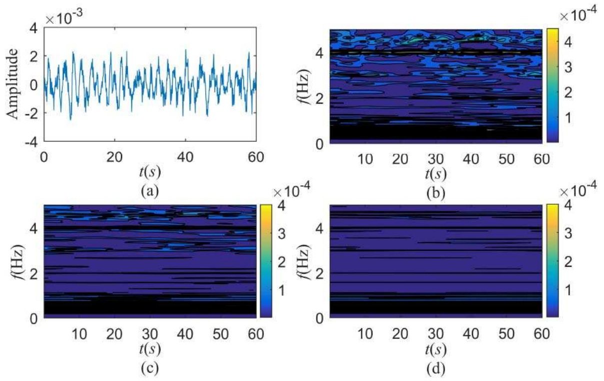

Fig. 3. The results of the DSD using FST under different window parameter $r$. The abscissa and ordinate represent sampling time and signal frequency respectively. (a) Target signal $t_w(n)$, (b) The FST with $r = 10$, (c) The FST with $r = 20$, (d) The FST with $r = 50$.

SG filter does not introduce signal time shift because it is based on the local least-squares polynomial and it has zero phase [19].

In SG filter, the local Least-squares Polynomial (LSP) fitting is first utilized to track fluctuations, and then the moving window can be used to segment signals [19]. $x(n)$ is denoted as frequency measurements of DSD. Concretely, for a local symmetry data window $n = [x_{-m}, x_{-m+1}, \ldots, x_0, \ldots, x_{m-1}, x_m]$ with a length $2M + 1$, where $m$ is the index of $n$, the common component of DSD under the window $n$ can be obtained as

$$l(n) = \sum_{k=0}^{k=p} b_k n^k \tag{1}$$

where $p$ denotes the order of a LSP ($p < 2M$), $b_k$ is the coefficient of polynomial. The goal of SG is to minimize the following error

$$\sum_{n=-M}^{n=M} [l(n) - x(n)] = \sum_{n=-M}^{M} \sum_{k=0}^{p} \Big(b_k n^k - x(n)\Big)^2 \tag{2}$$

After fitting the $x(n)$ using local window and LSP, the filtered frequency $t(n)$ can be obtained by subtracting the common data components $l(n)$ from the original data $x(n)$, namely $t(n) = x(n) - l(n)$.

To show the filtering effect, we randomly take a non-spoofed data of length 300 from the data set. The actual filtering results for DSD is shown in Fig. 2. This parameters of SG are an example. It can be seen from Fig. 2(a) that the trend of the frequency measurement in DSD is detected through SG filter. In Fig. 2(b), the target signal $t(n)$ is within 5 mHz, which indicates the common data component has been eliminated.

To reduce the computation before spatial fingerprint extraction, the $t(n)$ is divided into several signals of length $L_w$ using sliding windows where these truncated signals can be denoted as $t_w(n)$. The interval between different $t_w(n)$ is set to 100 sampling points.

### B. Time-Frequency Analysis Using Fast S-Transform

The multi-dimensional feature extraction of spoofing signal is the foundation for cyber-attack detection. Thus followed by the SG filter, the FST is used to extract spatial features via time-frequency analysis.

The calculation steps of FST can be summarized as: 1) The FFT of $t_w(n)$ and Gaussian window are calculated, denoting as $F(n)$ and $G(h)$ respectively, where the Gaussian window is part of the ST and can be used to adjust the resolution of signal. 2) For a specific DSD frequency point $q$, the spectrum of $F(n)$ is shifted to $F(n + q)$. Then we get the Hadamard product of $F(n+q)$ and $G(h)$, where the Hadamard product is element-wise product to get the same dimension as the input matrix [45]. 3) The inverse FFT are calculated to get the corresponding discrete time-frequency spatial fingerprint results $S(m, h)$ [23].

The result of FST is complex matrix. The magnitude of FST $A(m, h)$ can be expressed as $A(m, h) = |S(m, h)|$, where $m$ and $h$ denote the width and length of the matrix, respectively. To speed up the calculation, only one frequency point is calculated per two frequency points in FST [24]. Then the length of the spatial fingerprint $A(m, h/2)$ is further reduced to $A(m/2, h/2)$ by down sampling.

In FST, the Gaussian window parameter $r$ should have an appropriate value to get a desirable resolution. Thus, we analyze the time-frequency results of $t_w(n)$ under different parameters $r$. The spatial fingerprint $A(m/2, h/2)$ of the FST with different $r$ is depicted in Fig. 3. The color of the time-frequency results represent the amplitude, and the distribution of the time-frequency results represent the distribution of amplitude. We can choose the appropriate parameter value by comparing the time resolution and frequency resolution. The length of the sample $L_w$ is set to 600 in this test. The corresponding time-frequency matrix size is $m = 300$, $h = 600$, in which the DC component is ignored because the common frequencies have been eliminated. The actual results of the FST can be evaluated by the frequency resolution and time resolution [23].

As can be seen from the vertical axis of Fig. 3(b), the frequency information of $t_w(n)$ is very rich and the amplitude is scattered. From the attacker's point of view, to reproduce an illegible attack DSD, the same frequency components, frequency magnitude, start and end times need to be used. This means that copying the exact same DSD is very difficult due to the diversity of DSD. To choose the appropriate parameter value, for example, the amplitudes are randomly distributed in Fig. 3(b). It means a very low frequency resolution when $r = 10$. On the contrary, Fig. 3(d) has a very high frequency resolution because the frequency components are very clear from the y-axis perspective. However, the time resolution is very low with $r = 50$ because many frequency components are distributed throughout the time axis. Overall, Fig. 3(c) shows that the frequency components can be distinguished. It means that it has good frequency resolution. Compared with Fig. 3(d), the time resolution of Fig. 3(c) is higher because the time-generated nodes of different frequency components are clearer. In this paper, the window parameter $r$ is set to 20 as a compromise between time and frequency resolution for different dataset. The selected $r$ can be used to other DSD data set from different locations in the same power grid.

### *C. MCNN Model Training*

To realize the detection of spoofing attack, an effective classification method is required to authenticate the spatial fingerprints of incoming data. The MCNN is used to integrate spatial features and realize signal classification. The input data $A(m/2, h/2)$ is automatically filtered by MCNN, so that the information loss from the process of manual feature design can be avoided.

For general CNN, the structure of CNN contains three components: the convolutional layer, the pooling layer and full-connected (FC) layer [34]. The convolutional layer is used to extracted different features and learn the corresponding weights from the input data. The dimensions of the input and feature are downsampling using the pooling layer. Finally, the learned features are mapped to the outputs by combining multiple FC layers. By superimposing different layers on top of each other, higher-level features of spoofed data can be extracted. To briefly describe the principles of MCNN, we consider the single layer MCNN, which consists of one convolution layer and one pooling layer. For the input signal $A(m/2, h/2)$, the output of the convolution layer is defined as

$$C_i = g(w_i * A(m/2, h/2) + b_i) \tag{3}$$

where $w_i$ denotes the weight of the convolutional kernel in $i$-th feature map, the symbol * denotes the convolution operation, the function $g(\cdot)$ is the activation function. The function of the convolution kernel is to extract features from the input matrix. To prevent gradient disappearance, the Rectified Linear Unit (ReLU) is used as the activation function. The size of $C_i$ after the convolution layer is $d_c \times ((m/4-f_c)/s_c+1) \times ((h/4-f_c)/s_c + 1)$, where the $d_c$, $f_c$ and $s_c$ denote the depth, size of convolution kernel and stride respectively.

After the feature extraction of convolution layer, the max pooling layer is utilized to filter out redundant feature information. The output of max pooling layer can be expressed as

$$P_i\big(f_p\big) = \max\big\{0, C_i|_{f_p\times f_p}\big\} \tag{4}$$

where $f_p$ denotes the size of pooling layer. The $P_i$ means that the max value between 0 and zone $[f_p, f_p]$ in $C_i$.

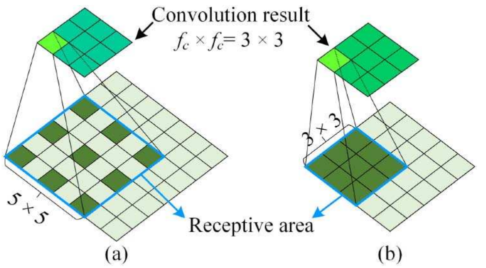

Fig. 4. Different convolution operations with convolution kernel size $f_c \times f_c = 3 \times 3$. (a) Dilated convolution with $\gamma = 2$, (b) Standard convolution with $\gamma = 1$.

Then, the $P_i$ is flatted at full connected layer and the output of full connected layer $F$ is fed to the categorical cross entropy function to training [35]. The DSD is then detected by the softmax function, which can be expressed as

$$S(F) = e^{F_j} / \sum_{i=1}^{Q} e^{F_i} \tag{5}$$

where $i = 1, 2, \ldots, Q$, $Q$ is the total number of DSD class. Generally, the class of the maximum probability value in $S(F)$ is the category to which the DSD belongs.

Additionally, in order to increase the diversity of features, the dilated convolution is used to expand the receptive area [32]. It have been shown that the dilated convolution view is more flexible than the standard convolution kernel, as shown in Fig. 4. It can be seen from Fig. 4(a) that the dilated factor $\gamma$ determines the size of the receptive view and a higher $\gamma$ means a larger receptive view. The receptive area of dilated convolution and standard convolution are is $5 \times 5$ and $3 \times 3$ respectively when the kernel size is $f_c \times f_c = 3\times 3$. Thus, we further propose the MCNN to combine the advantages of two convolution operations, which the dilated convolution and standard convolution kernel are used in the same layer. The principle of dilated convolution can be expressed as

$$C_i^{\gamma} = g\big(w_i *_{\gamma} A(m/2, h/2) + b_i\big) \tag{6}$$

where the $*_{\gamma}$ denotes the dilated convolution with dilated factor. The receptive field length of dilated convolution is $(f_c - 1) \times \gamma + 1$. For the convolution layer with depth of $d_c$, half of the convolution operation of $d_c$ adopts standard convolution and the other half is dilated convolution in this paper. Therefore, the output of the convolutional layer is

$$C_{\gamma i} = \big[0.5C_i, 0.5C_i^{\gamma}\big] \tag{7}$$

It shows that the depth of $d_c$ is composed of two parts, $C_i^{\gamma}$ and $C_{\gamma i}$, which means that the features are more diversified. Then the parameters of MCNN are trained and optimized by backpropagation algorithms after establishing the MCNN structure. Finally, the spoofed data can be detected according to the softmax function in Equation (5).

### *D. Data Spoofing Cyber-Attack Using Threshold Criterion*

To realize cyber-attack and data spoofing detection, a threshold $T_{s(f)}$ is required to distinguish the attacked DSD and normal DSD, which is considered as attack behavior when

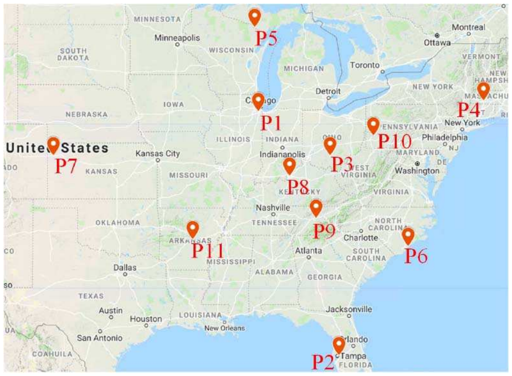

Fig. 5. The map of distribution synchrophasor locations.

the probability value $S(F)$ is lower than $T_{s(f)}$. To selected the threshold $T_{s(f)}$, a CI threshold criterion is further proposed.

After training the MCNN model, the $T_{s(f)}$ is obtained by balancing the accuracy of spoofed data detection and normal DSD authentication. Broadly, a detection accuracy "trade off" should be considered when choosing the $T_{s(f)}$. If a too large value is selected for $T_{s(f)}$, all the DSD can be identified as spoofed data. Conversely, the spoofed data cannot be accurately identified when $T_{s(f)}$ is set to a too low value. To select a suitable $T_{s(f)}$, a CI reference guideline is designed for $T_{s(f)}$, which can be obtained as

$$\mathrm{CI} = Max \ \left[0.5\sum(1-\lambda)A_{at}(\lambda) + 0.5\sum N_{at}(\lambda) - \left|y''\right|\right]_{T_{s(f)}}$$
$$s.t. \ \ y'' = \left(0.5\sum(1-\lambda)A_{at}(\lambda) + 0.5\sum N_{at}(\lambda)\right)'' \quad (8)$$

where the $A_{at}(\lambda)$ and $N_{at}(\lambda)$ denote the Average Accuracy ($A_a$) for spoofed data detection and the Non-spoofed data Accuracy ($N_a$) for normal data under different threshold $T_{s(f)}$, respectively. The third item $y'' = y_{u+2} - 2y_{u+1} + y_u$ is the second order difference, where $u$ is the index under different threshold. The second order difference term is used to constrain the CI value to choose a smooth threshold point. The equation represents that the max value is elected from different data spoofing ratio λ. The data spoofing ratio λ is used to define the strength of the attack

$$\lambda = L_a/L_w \quad (9)$$

where the $L_a$ and $L_w$ are the length of attack and raw data, respectively. Finally, it indicates that the sum of $A_a$ and $N_a$ is large and stable when Equation (5) is taken to the maximum. Concretely, a $T_{s(f)}$ between 0.5 and 1 is specified through experimental analysis.

## V. Visual Analysis of Features

In this paper, the DSD from 11 different locations (P1-P11) in Frequency measurement Network (FNET/Grideye) system [36] are used. Fig. 5 shows the geographical locations of DSD in our study. It shows that the PMUs are distributed in various regions. The DSD of these nine locations are collected to verify the validity of the proposed framework. There are 12,800 samples used in validation for DSD in each location with 10 Hz reporting rate in Fig. 5.

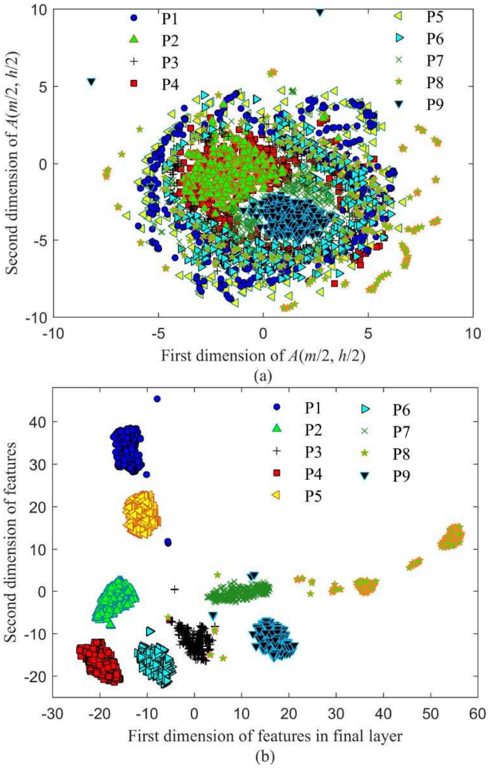

Fig. 6. Visualizations of the input time-frequency matrix signal $A(m/2, h/2)$ and features in the final layer of MCNN by t-SNE. (a) Visualizations of the input $A(m/2, h/2)$, (b) Visualizations of features in the final layer of MCNN.

### A. Visualization of Classification Capability

In order to verify the feature extraction ability of MCNN, a nonlinear dimension reduction technique called t-Distributed Stochastic Neighbor Embedding (t-SNE) is used to visualize high-dimensional data [37]. In t-SNE, the clustering degree of features reflects the classification performance.

The input signal $A(m/2, h/2)$ and corresponding output features in the final layer are fed to t-SNE. 300 samples per synchrophasor class are used for visualization. The perplexity and the number of iterations are set to 40 and 4000 respectively in t-SNE. The visualization of the different data are shown in Fig. 6. The markers represents the degree of aggregation of the input data, where the dimensions of input data are changed to 2 after transformed by t-SNE.

It is observed from Fig. 6(a) that the input spatial fingerprints overlap each other, making it difficult to distinguish the DSD in different locations. In the Fig. 6(b), all the DSD have been separated from each other after being processed by MCNN. The spatial fingerprints of the same location are gathered together. In addition, the spatial fingerprint of P1 and P8 are more dispersed, indicating that these spatial fingerprints contain multiple signal components. It reveals from Fig. 6 that MCNN can identify the difference of DSD from multiple locations.

### B. Feature Visualization

To further explore the features learned by MCNN, we visualize the output features of different layers. By observing the

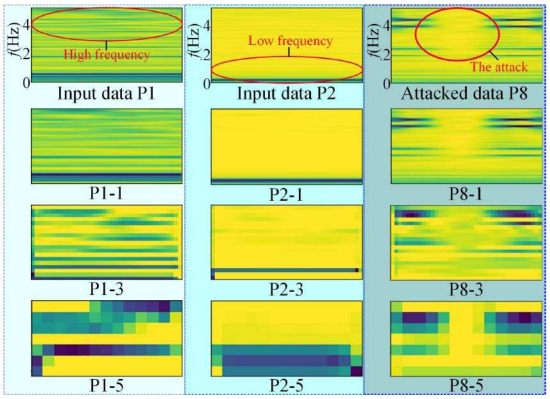

Fig. 7. Visualization of multiple randomly selected features in different layers of MCNN. The P*r*-*i* represents the features of P*r* locations from the *i*th layer.

shape of spatial fingerprint, it is beneficial to improve the model through continuous feedback and adjustment.

First, we build a MCNN with five layers. To simplify the model, all the size of convolution kernel is set to $f_c = 3$ and the depth of convolution layer is $d_c = 8$ per layer. The size of the pooled layer is set to $f_p = 2$. We randomly selected the raw DSD from three locations, P1, P2, and P8. To simulate the spoof attack, the DSD in P8 is tampered by the DSD in P2.

Fig. 7 exhibits the features from the first, third and the fifth layers. It shows that the P1 contains components of different frequencies from 0-5 Hz, P2 contains only low-frequency components ($f < 2$ Hz) and P8 has a small amount of high-frequency components ($f > 2$ Hz). It can be seen from Fig. 7 that the features of the first layer are close to the original input signal, indicating that MCNN does not learn any useful information. However, the low-frequency information is extracted in the third layer as can be seen from P2-3 and P8-3. In the fifth layer, the low frequency component is completely extracted for P2-5. Additionally, the features of the high frequency portion of P1 and P8 are extracted by P1-5 and P8-5. Particularly, for the attacked data P8 and P8-5, it shows that the location of the attack is determined, and the attack effect becomes prominent as the number of convolution layers increases. Thus, it is evident that the CNN has the potential ability to detect spoofed data.

## VI. Model Performance Assessment

To verify the effectiveness of the proposed method, the DSD samples from multiple locations in Fig. 5 are used for verification. There are 12,800 different samples used for DSD with 10 Hz reporting rate. The DSD from P1-P9 is randomly assigned to different sets, of which 70% are used for training, 15% for testing and 15% for verification. The cross validation method is applied to validate the model. The DSD from P10 and P11 are not used during MCNN training process thus are reserved as the attack signal source. It is worth mentioning that the MCNN is only trained using the non-spoofed DSD from nine locations (P1-P9). To prevent over-fitting, the dropout technique and training technic are adopted in MCNN [38]. For the dropout, we denote the $\rho$ as the ratio of remaining nodes in MCNN. Grid search method is used to determine classifier parameters [39]. Additionally, the learning rate would be reduced by half when the loss value does not decrease for 5 consecutive iterations. The implementation of MCNN is based on the Keras framework on a PC with GPU GTX 1060, which the Keras is a deep learning library [40].

TABLE I
The Parameter Settings of the SG and FST

| Method | SG | | FST |
|---|---|---|---|
| Parameter | $p$ | $M$ | $r$ |
| Value | 3, 4 | [50, 75] | 20 |

### A. Parameter Sensitivity Analysis

Since parameters of the model directly affect the accuracy of the spoofing detection, the appropriate parameters are significant to the performance of the proposed method.

To select appropriate SG filter parameters, Fig. 8 presents the results of the SG filter for the DSD at P1 with different $p$ and $M$. It can be seen from Fig. 8(a) that the SG filter fails to capture some trends in waveform when $p = 1$. On the contrary, the SG filter with order $p = 5$ varies dramatically indicates that the common components were not learned. The SG filter shows a balance between computational complexity and efficiency when $p = 3$. Thus, the polynomial order $p$ is set to 3 or 4 to get a better filtering performance and avoid overfitting.

As can be noticed from Fig. 8(b) that a higher window width $M (M \geq 100)$ prevents the SG filter from capturing detailed trends in the waveform. However, a smaller window width $M$ results in an inefficient filtering when $M = 25$. Consequently, a small range of parameters, i.e., $M \in [50, 75]$, is selected to apply to the DSD after some trial and error. The detailed parameter settings of SG and FST are summarized in Table I. Therefore, the SG parameters of different locations can be selected from Table I according to the actual filtering effect.

On the other hand, the number of layers and size of convolution kernel have a great impact on the performance of MCNN. To obtain the optimal number of convolution layers, the non-spoofed DSD is used to verify parameter sensitivity in the training process.

To select appropriate MCNN parameters, Fig. 9 shows the relationship between authentication accuracy of raw data, the number of convolution layers and convolution kernel size using grid search. For different MCNN structures, all the nodes of the full connected layer are set to 300. To keep the parameter capacity of MCNN at a similar level, the size of pooling are set to 2, 3, 4, 5 for MCNN-5, MCNN-4, MCNN-3 and MCNN-2 respectively, where the MCNN-*i* represents that the number of convolution layer is equal to *i*. The other parameters of MCNN are set the same to have a fair comparison.

It demonstrates that the MCNN has the highest recognition accuracy when the convolution kernel size is 3×3. The accuracy of source identification decreases slightly as the size of convolution kernel increases. Additionally, it shows that the layer number of MCNN also affects the accuracy. Overall, the MCNN-3 performs better than other models.

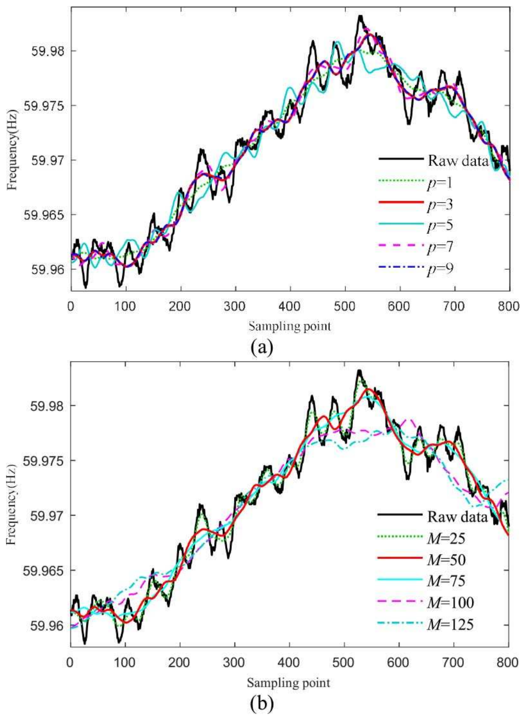

Fig. 8. Results of SG filter with different parameters $p$ and $M$. (a) Filtering results under different polynomial order $p$ when $M = 50$, (b) Filtering results under different window width $M$ when $p = 4$.

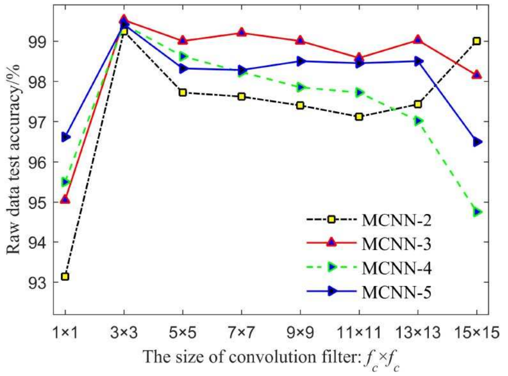

Fig. 9. The raw data authentication performance of MCNN for non-spoofed data under different layers and convolution kernel sizes.

In this work, a MCNN with three convolution layers is selected based on the above parameter analysis, and the size of all the convolution kernels are set to 3×3. The detailed parameter structure of MCNN is listed in Table II. The stride $s_c$ of convolution layer is set to 1. The dropout layer is placed after the fully connected layer, and the parameter of dropout $\rho$ is set to 0.5. The dilated factor $\gamma$ is set to 2. The batch size of the training is set to 256. The model parameters are trained using the RMSProp optimizer. The total number of parameters in MCNN is nearly 220, 000.

### B. Attack Detection of Synchrophasor Data

To verify the accuracy of the proposed method for attack detection, a spoofing method that directly tampers the original DSD is adopted [25]. In the verification data set, the DSD is randomly spoofed by the DSD from other locations.

TABLE II
STRUCTURE OF MCNN FOR DSD ATTACK DETECTOPM

| Layer | Layer 1 | Layer 2 | Layer 3 | Layer 4 |
|---|---|---|---|---|
| Conv. | 8×3×3 | 16×3×3 | 16×3×3 | - |
| Pooling | 3×3 | 4×4 | 3×3 | - |
| FC | - | - | - | 300 |

It is reported that the format of convolution is $d_c$×$f_c$×$f_c$, and the format of pooling is $f_p$×$f_p$.

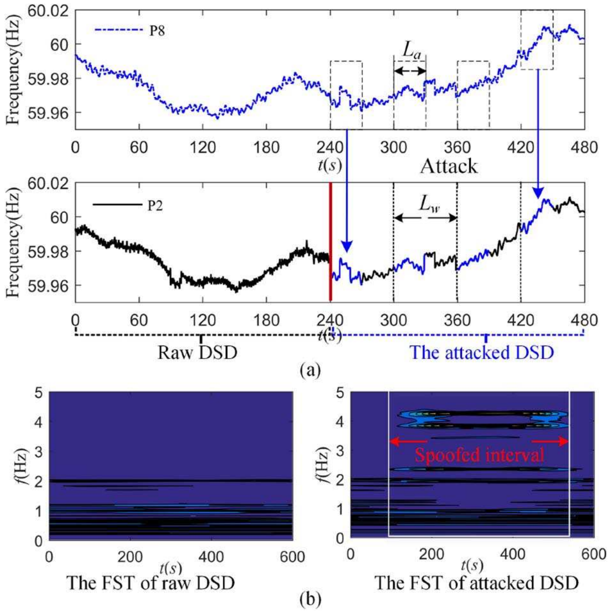

Fig. 10. Illustration of DSD data attack. (a) A schematic diagram of DSD data attack, where the DSD in P2 is spoofed by data in P8, (b) The FST of the raw DSD and attacked DSD.

In this work, we randomly test four kinds of attacks, in which the DSD in one location is spoofed by data in another location with same timestamp. The $L_w$ is set to 600, which is equivalent to 1 minute data length. The illustration of data attack and corresponding spatial fingerprints are shown in Fig. 10. For each sample, it can be observed from Fig. 10(a) that a portion of the original DSD is attacked. As can be seen from Fig. 10(b), the FST can potentially identify the components of the signal at different times due to the different frequency components of DSD in each location. Therefore, such attacking characteristics can then be captured by MCNN.

To identify the attack behavior, the threshold of softmax function is adjust through Equation (5). When the value of $S(F)$ is lower than the threshold $T_{s(f)}$, it can be considered that the attack has occurred. The performance of four different spoofed data recognition experiments under different $T_{s(f)}$ and $\lambda$ is depicted in Fig. 11. The step size of $T_{s(f)}$ and $\lambda$ are set to 0.02 and 1/12 respectively.

It can be observed that all the recognition accuracy of the attack increases with $\lambda$. When $\lambda$ is greater than 3/12, more than 90% of attacks can be detected in Fig. 11(a) and (b). Similarly, the reduction of the $T_{s(f)}$ makes the recognition accuracy of the attack decrease. For example, the recognition accuracy is lower than 94% when $T_{s(f)}$ is lower than 0.9 as shown in Fig. 11(d). It also shows that the model has the lowest detection accuracy when $\lambda \leq 2/12$ and the $T_{s(f)} \leq 0.96$. Particularly, the accuracy

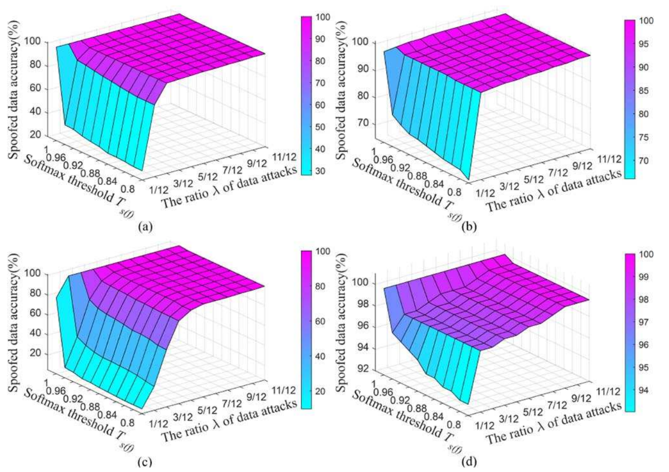

Fig. 11. Spoofed data recognition accuracy under different softmax threshold $T_{s(f)}$ and λ. (a) The DSD in P4 is spoofed by data in P9, (b) The DSD in P4 is spoofed by data in P8, (c) The DSD in P2 is spoofed by data in P5, (d) The DSD in P2 is spoofed by data in P8.

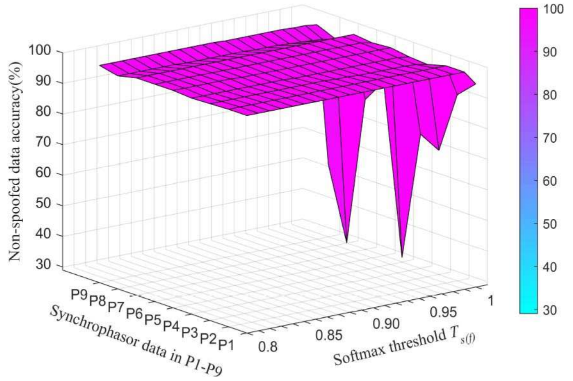

Fig. 12. The non-spoofed DSD recognition accuracy when the $T_{s(f)}$ is range from 0.8 to 1.

reaches 100% when the $T_{s(f)}$ close to the maximum value $S(F)_{\max}$ [the $S(F)_{\max}$ is 1 in this test], indicating that some normal DSD is misidentified.

The recognition accuracy of non-spoofed DSD with different $T_{s(f)}$ is shown in Fig. 12. It shows that the performance of non-spoofed data decreases rapidly when the threshold is set to 1. On the contrary, the accuracy of non-spoofed data is relatively stable for each location when the $T_{s(f)}$ range is between 0.8 and 0.95. Therefore, it is reasonable to set the threshold to less than 1. Taking the above results into account, we set $T_{s(f)}$ for 0.92 in P2 according to Equation (5) as a compromise between attack detection and non-spoofed DSD recognition. Thresholds for other locations can be set in the similar approach.

To further verify the spoofed accuracy, two unknown attacks (both outside the model training set) are used, of which the DSD is spoofed by the DSD from P10 and P11. The Average Accuracy (AA) is the average rate for attack detection at different λ. The AA results of two unknown attacks with different λ are shown in Fig. 13. It can be seen from Fig. 13(b) that the average AA reached 92.35 % when $T_{s(f)}$ is set by the proposed CI threshold criterion. These two unknown attacks have the same trend as Fig. 11, indicating that the proposed algorithm has the ability to detect unknown spoofed signals.

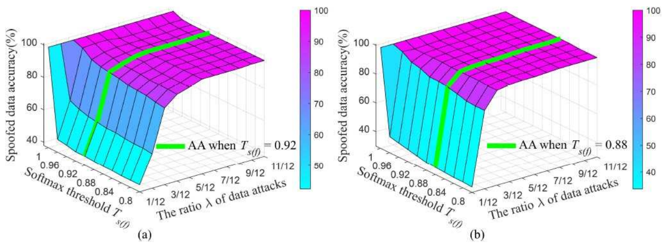

Fig. 13. The spoofed DSD recognition accuracy using non-training data set. (a) The DSD in P2 is spoofed by data in P11, the average AA is 89.73 % when $T_{s(f)} = 0.92$. (b) The DSD in P4 is spoofed by data in P10, the average AA is 92.35 % when $T_{s(f)} = 0.88$.

TABLE III
PERFORMANCE COMPARED UNDER DIFFERENT STEPS

| Method | Classifier structure | Time (s) | $M_r$ (%) | $A_a$ (%) |
|---|---|---|---|---|
| LSTM | One layer LSTM | 7.01 | 21.06 | 87.26 |
| SG-LSTM | One layer LSTM | 7.07 | 19.03 | 85.42 |
| 1DCNN | Five-layer 1D conv. layer | 0.74 | 11.40 | 86.54 |
| SG-1DCNN | Five-layer 1D conv. layer | 0.80 | 7.83 | 79.50 |
| FST-MCNN | Three-layer conv. layer | 9.57 | 2.28 | 81.26 |
| SD-FST-CNN | Three-layer conv. layer | 9.14 | 0.61 | 89.71 |
| **Proposed method** | **Three-layer conv. layer** | **9.61** | **0.18** | **91.46** |

Note: $M_r$(%): Misidentification Rate for non-spoofed data.
$A_a$(%): Average Accuracy for spoofed data detection.

### C. Performance Comparison

To verify the contribution of FST and SG in the proposed method, FST and SG steps are removed separately. It should be note that a 1-Dimensional Convolutional Neural Network (1DCNN) is used for direct detection since the data dimension becomes one-dimensional when FST is removed [41]. The main difference between 1DCNN and MCNN is the dimension of convolution kernel. Meanwhile, the Long Short Term Memory (LSTM), a kind of time series process method [42], is also used to compare with the proposed method. The number of nodes and layers of LSTM are optimized selected as 50 and 1 respectively. The inputs of 1DCNN and LSTM are the raw non-spoofed DSD. The input of SG-1DCNN are data from which the common component is removed by SG. The number of layers are optimally selected using grid search.

Table III shows that the both the $M_r$ and $A_a$ accuracy of LSTM and SG-LSTM are lower than the proposed method. The time consuming of LSTM is larger than 1DCNN. It is demonstrated that the proposed method is 11% higher than the 1DCNN method according to the $M_r$ result. Meanwhile, it can be inferred that the time of SG is about 0.05 seconds for all the 1920 verification samples. The average time taken for the SG step for each sample is approximately 0.025 milliseconds. Therefore, it can be concluded that the SG step does not significantly affect the real-time performance. Based on the 1DCNN and SG-1DCNN, the $M_r$ and $A_a$ results show that the common component removed by SG does not affect the identification accuracy of DSD. Compared with SG+1DCNN and FST-MCNN, the $M_r$ and $A_a$ results demonstrate that FST helps

TABLE IV
PERFORMANCE COMPARED TO OTHER METHODS

| Method | Classifier structure | Time (s) | $M_r$ (%) | $A_a$ (%) |
|---|---|---|---|---|
| SG-FST-SVM | Linear kernel function | 10.50 | 0.79 | 86.53 |
| SG-FST-ANN | 45000-1000-300 | 8.65 | 1.55 | 83.52 |
| SG-FST-SAE | 45000-600-300-600-45000 | 8.76 | 2.95 | 89.50 |
| **Proposed method** | **Three-layer conv. layer** | **9.61** | **0.18** | **91.46** |

Note: $M_r$(%): Misidentification Rate for non-spoofed data.
$A_a$(%): Average Accuracy for spoofed data detection.

feature extraction because the spatial fingerprints of different DSD can be extracted. It can be seen that the proposed method has the highest $A_a$ and lowest $M_r$. The reason is that the diversity of features in MCNN contribute to cyber-attack detection. Compared with the proposed method and SG-FST-CNN, it can be seen that the MCNN can improve the attack recognition result by 1.75% under the premise of slightly increasing the calculation amount.

To further verify the validity of MCNN, we compare the proposed method with some common machine learning methods, including Support Vector Machine (SVM), Artificial Neural Network (ANN) and Stacked Auto-Encoder (SAE) [43], [44]. For these methods, the input spatial fingerprint $A(m/2, h/2)$ is reshaped to accommodate the one-dimensional input. The parameters of these methods are optimally selected using grid search.

The details of compared spoofing detection methods are as follows:

1) SG-ST-SVM: The linear kernel and stochastic gradient descent are used to solve SVM. The kernel coefficient are optimally screened from 0.01 to 0.001, and finally 0.041 is selected.
2) SG-ST-ANN: A 2-layer ANN is used for classification. For simplicity, the activation function RELU and softmax classifier are used in ANN. The total number of parameters is about 45 million.
3) SG-ST-SAE: The softmax classifier is used to classify in SAE with total model parameters 54 million.

The classifier structure, non-spoofed DSD identification and attack detection results of different methods are listed in Table IV. The proposed MCNN model is offline trained and used for real-time DSA detection. The running time is recorded for efficiency comparison. The running time of MCNN is slightly higher than ANN and SAE. However, the average time of each sample is 5 milliseconds, thus the real-time monitoring can be satisfied considering 1 min data window for input samples. It is noted that both ANN and SAE models have tens of millions of parameters, which can easily lead to overfitting. It shows that the SVM and MCNN have similar Mr. However, the SVM are more time-consuming. The ANN and SAE consume less time but the performance of $A_a$ does not exceed 90%. Compared to these machine learning methods, the proposed method has the lowest $M_r$ for non-spoofed data and best performance for attack detection because the feature extraction ability of MCNN is stronger.

TABLE V
PERFORMANCE COMPARISON WITH TWO RECENT STUDIES

| Method | Number of categories | Feature extraction | $M_r$ (%) | $A_a$ (%) |
|---|---|---|---|---|
| MM-TF-RFC [25] | 10 | manual | 3.60 | 72.00 |
| WT-FFT-ANN [16] | 5 | automatic | 3.26 | 87.12 |
| Proposed method | 9 | automatic | 0.18 | 91.46 |

Note: $M_r$(%): Misidentification Rate for non-spoofed data.
$A_a$(%): Average Accuracy for spoofed data detection.

We further compare the proposed method with two machine learning-based methods on DSD spoofing attack detection in [16] and [25], including the Mathematical Morphology (MM)-Time-Frequency (TF)-Random Forest Classification (RFC) and Wavelet Transform (WT)-Fast Fourier Transform (FFT)-ANN. The result is listed in Table V, which demonstrates that the performance of proposed method with highest $A_a$ and lowest $M_r$ is superior compared with the methods in the literatures. Since manual features are prone to information loss, it can be also concluded that the performance of automatic feature extraction are better than the conventional manual extraction in [25]. Compared with the method in [16] and proposed framework, it shows that the classification ability of traditional ANN is not as good as MCNN. To ensure the reliability of the model, the parameter of the model can update daily using the latest DSD.

## VII. CONCLUSION

In this paper, a fingerprint-based SG-FST-MCNN framework is proposed to identify the source of the DSD and detect data spoofing cyber-attack, which can be summarized into four steps:

1) The SG filter is first utilized to eliminate the common component of DSD from multiple locations; 2) To effectively extract spatial fingerprint, the FST is applied on the output of SG filter for spatial fingerprint extraction via time-frequency analysis; 3) Utilizing the dilated convolution and standard convolution, a MCNN is proposed to classify spatial fingerprint automatically, which can avoid interference in manual feature selection; 4) To distinguish the raw DSD and spoofing DSD, the CI threshold criterion is proposed to detect the data spoofing cyberattack.

By implementing this framework, the common trend component of DSD is effectively removed. The spoofing behavior in DSD can be captured via FST based on the feature visualization experiments. Particularly, the visualization of classification capability exhibits the meaning of feature extraction and verify the classification ability of MCNN. Using the actual non-spoofed DSD in FNET/Grideye, the attacked experiments demonstrates the superiority of the proposed framework in the aspects of interpretability and automatic extraction. The accuracy for DSD spoofing detection of proposed method is higher than some advanced machine learning methods. It should be noted that the performance of attack detection degrades as the data spoofing ratio λ decreases, especially when $\lambda < 10\%$. Meanwhile, the DSD samples are collected from different cities with large geographical distance. The DSD with small distance and high similarity such as same city has not been verified. Thus, the next step is to enhance this approach for the condition of low λ and DSD with higher similarity.

## References

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

[2] S. Xu, H. Liu, T. Bi, and K. E. Martin, "A high-accuracy phasor estimation algorithm for PMU calibration and its hardware implementation," *IEEE Trans. Smart Grid*, early access, doi: 10.1109/TSG.2020.2965195.

[3] S. Pal, B. Sikdar, and J. H. Chow, "An online mechanism for detection of gray-hole attacks on PMU data," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2498–2507, Jul. 2018.

[4] C. Beasley, X. Zhong, J. Deng, R. Brooks, and G. K. Venayagamoorthy, "A survey of electric power synchrophasor network cyber security," in *Proc. IEEE PES Innov. Smart Grid Technol. Europe Istanbul*, 2014, pp. 1–5.

[5] S. Mohagheghi, "Integrity assessment scheme for situational awareness in utility automation systems," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 592–601, Mar. 2014.

[6] K. Wang, M. Du, S. Maharjan, and Y. Sun, "Strategic honeypot game model for distributed denial of service attacks in the smart grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2474–2482, Sep. 2017.

[7] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[8] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2444–2453, Sep. 2015.

[9] S. Sridhar and G. Manimaran, "Data integrity attack and its impacts on voltage control loop in power grid." in *Proc. IEEE Power Energy Soc. Gen. Meeting*, San Diego, CA, USA, Jul. 2011, pp. 1–6.

[10] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "Analysis of IEEE C37.118 and IEC 61850-90-5 synchrophasor communication frameworks," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Boston, MA, USA, 2016, pp. 1–5.

[11] J. F. K. Stouffer and K. Kent, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*, document SP 800-82, Nat. Inst. Stand. Technol., Gaithersburg, MA, USA, Sep. 2006.

[12] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580–591, Mar. 2014.

[13] Y. Guo, C. Ten, and P. Jirutitijaroen, "Online data validation for distribution operations against cybertampering," *IEEE Trans. Power Syst.*, vol. 29, no. 2, pp. 550–560, Mar. 2014.

[14] M. Yue, T. Hong, and J. Wang, "Descriptive analytics based anomaly detection for cybersecure load forecasting," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 5964–5974, Nov. 2019.

[15] M. Zhou, Y. Wang, A. K. Srivastava, Y. Wu, and P. Banerjee, "Ensemble-based algorithm for synchrophasor data anomaly detection," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2979–2988, May 2019.

[16] W. Yao *et al.*, "Source location identification of distribution-level electric network frequency signals at multiple geographic scales," *IEEE Access*, vol. 5, pp. 11166–11175, 2017.

[17] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Trans. Ind. Informat.*, vol. 13, no. 1, pp. 198–207, Feb. 2017.

[18] Y. Cui, F. Bai, Y. Liu, and Y. Liu, "A measurement source authentication methodology for power system cyber security enhancement," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3914–3916, Jul. 2018.

[19] J. Seo, H. Ma, and T. K. Saha, "On Savitzky–Golay filtering for online condition monitoring of transformer on-load tap changer," *IEEE Trans. Power Del.*, vol. 33, no. 4, pp. 1689–1698, Aug. 2018.

[20] M. Sahani and P. K. Dash, "Automatic power quality events recognition based on Hilbert Huang transform and extreme learning machine," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 3849–3858, Sep. 2018.

[21] P. D. Achlerkar, S. R. Samantaray, and M. S. Manikandan, "Variational mode decomposition and decision tree based detection and classification of power quality disturbances in grid-connected distributed generation system," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3122–3132, Jul. 2018.

[22] N. Ma and D. Wang, "Extracting spatial–temporal characteristics of frequency dynamic in large-scale power grids," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 2654–2662, Jul. 2019.

[23] M. Biswal and P. K. Dash, "Measurement and classification of simultaneous power signal patterns with an S-transform variant and fuzzy decision tree," *IEEE Trans. Ind. Informat.*, vol. 9, no. 4, pp. 1819–1827, Nov. 2013.

[24] M. V. Reddy and R. Sodhi, "A modified S-transform and random forests-based power quality assessment framework," *IEEE Trans. Instrum. Meas.*, vol. 67, no. 1, pp. 78–89, Jan. 2018.

[25] Y. Cui, F. Bai, Y. Liu, P. Fuhr, and M. E. Morales-Rodriguez, "Spatio-temporal characterization of synchrophasor data against spoofing attacks in smart grids," *IEEE Trans. Smart Grid*. vol. 10, no. 5, pp. 5807–5818, Sep. 2019.

[26] J. Landford *et al.*, "Fast sequence component analysis for attack detection in smart grid," in *Proc. 5th Int. Conf. Smart Cities Green ICT Syst. (SMARTGREENS)*, Rome, Italy, 2016, pp. 1–8.

[27] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1644–1652, Sep. 2017.

[28] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 8, pp. 1773–1786, Aug. 2016.

[29] S. Wang and H. Chen, "A novel deep learning method for the classification of power quality disturbances using deep convolutional neural network," *Appl. Energy*, vol. 235, pp. 1126–1140, Feb. 2019.

[30] K. Chen, J. Hu, and J. He, "Detection and classification of transmission line faults based on unsupervised feature learning and convolutional sparse autoencoder," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1748–1758, May 2018.

[31] H. Liu, F. Hussain, Y. Shen, S. Arif, A. Nazir, and M. Abubakar, "Complex power quality disturbances classification via curvelet transform and deep learning," *Elect. Power Syst. Res.*, vol. 163, pp. 1–9, Oct. 2018.

[32] N. Lessmann *et al.*, "Automatic calcium scoring in low-dose chest CT using deep neural networks with dilated convolutions," *IEEE Trans. Med. Imag.*, vol. 37, no. 2, pp. 615–625, Feb. 2018.

[33] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370–379, Dec. 2014.

[34] P. Li, Z. Chen, L. T. Yang, Q. Zhang, and M. J. Deen, "Deep convolutional computation model for feature learning on big data in Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 790–798, Feb. 2018.

[35] F. Yu and V. Koltun, "Multi-scale context aggregation by dilated convolutions," 2016. [Online]. Available: arXiv:151107122v2.

[36] Y. Liu *et al.*, "Wide-area-measurement system development at the distribution level: An FNET/grideye example," *IEEE Trans. Power Del.*, vol. 31, no. 2, pp. 721–731, Apr. 2016.

[37] L. van der Maaten and G. Hinton, "Visualizing data using t-SNE," *J. Mach. Learn. Res.*, vol. 9, pp. 2579–2605, Nov. 2008.

[38] N. Srivastava, G. Hinton, and A. Krizhevsky, "Dropout: A simple way to prevent neural networks from overfitting," *J. Mach. Learn. Res.*, vol. 15, no. 1, pp. 1929–1958, 2014.

[39] D. Chicco, "Ten quick tips for machine learning in computational biology," *Bio Data Min.*, vol. 10, p. 35, Dec. 2017.

[40] D. Chollet. (2015). *GitHub Repository*. [Online]. Available: https://github.com/keras-team/keras

[41] S. Wang and H. Chen, "A novel deep learning method for the classification of power quality disturbances using deep convolutional neural network," *Appl. Energy*, vol. 235, pp. 1126–1140, Feb. 2019.

[42] H. Palangi *et al.*, "Deep sentence embedding using long short-term memory networks: Analysis and application to information retrieval," *IEEE/ACM Trans. Audio, Speech, Language Process.*, vol. 24, no. 4, pp. 694–707, Apr. 2016.

[43] K. Chen, J. Hu, and J. He, "A framework for automatically extracting overvoltage features based on sparse autoencoder," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 594–604, Mar. 2018.

[44] S. Khokhar, A. A. B. M. Zin, A. S. B. Mokhtar, and M. Pesaran, "A comprehensive overview on signal processing and artificial intelligence techniques applications in classification of power quality disturbances," *Renew. Sustain. Energy Rev.*, vol. 51, pp. 1650–1663, Nov. 2015.

[45] S. Cao, Z. Ye, D. Xu, and X. Xu, "A Hadamard product based method for DOA estimation and gain-phase error calibration," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 2, pp. 1224–1233, Apr. 2013.

**Wei Qiu** received the B.Sc. degree in electrical engineering from the Hubei University of Technology, Wuhan, China, in 2015, and the M.Sc. degree in electrical engineering from Hunan University, Changsha, China, in 2017, where he is currently pursuing the Ph.D. degree with Hunan University.

He is also a joint Doctoral student with the University of Tennessee from 2019. His current research interests include power system analysis and monitoring, power quality measurement, and reliability analysis of power equipment.

**Qiu Tang** received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from Hunan University, Changsha, China, in 1992, 1995, and 2010, respectively, and the M.Sc. degree in electrical engineering from the University of Nottingham, Nottingham, U.K., in 2005.

She has been an Associate Professor with Hunan University since 2006. Her current research interests include power system analysis, digital signal processing, and virtual instruments.

**Yajun Wang** (Member, IEEE) received the B.Sc. and M.Sc. degrees from the School of Electrical Engineering, Wuhan University, Wuhan, China, in 2012 and 2014, respectively, and the Ph.D. degree in electrical engineering from the University of Tennessee, Knoxville, TN, USA, in 2019.

She is currently working with Dominion Energy Virginia, Richmond, VA, USA, as a Senior Power System Engineer. Her research interests are big data analytics, power system stability and control, system restoration, energy storage system, electric vehicle, and DER integration.

**Lingwei Zhan** (Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Tongji University in 2008 and 2011, respectively, and the Ph.D. degree from the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, in 2015.

He is currently a R&D Staff with Oak Ridge National Laboratory. His research interests include advanced grid sensors, PMU, synchrophasor measurement algorithm, wide-area power system monitoring, renewable energy sources, FACTs, and HVDC.

**Yilu Liu** (Fellow, IEEE) received the B.S. degree from Xian Jiaotong University, China, and the M.S. and Ph.D. degrees from Ohio State University, Columbus, in 1986 and 1989, respectively.

She was a Professor with Virginia Tech. She is currently the Governor's Chair with the University of Tennessee (UTK), Knoxville, and Oak Ridge National Laboratory (ORNL). She is elected as the Member of National Academy of Engineering in 2016. She is also the Deputy Director of the DOE/NSF-cofunded Engineering Research Center CURENT. She led the effort to create the North American power grid Frequency Monitoring Network, Virginia Tech, which is currently operated with UTK and ORNL as GridEye. Her current research interests include power system wide-area monitoring and control, large interconnection-level dynamic simulations, electromagnetic transient analysis, and power transformer modeling and diagnosis.

**Wenxuan Yao** (Member, IEEE) received the B.S. and Ph.D. degrees from the College of Electrical and Information Engineering, Hunan University, Changsha, China, in 2011 and 2017, respectively, and the Ph.D. degree from the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, USA, in 2018.

He is currently a Research Associate with Oak Ridge National Laboratory. His research interests include wide-area power system monitoring, synchrophasor measurement application, embedded system development, power quality diagnosis, and big data analysis in power systems.