Detection of Synchrophasor False Data Injection Attack Using Feature Interactive Network

Wei Qiu, *Graduate Student Member, IEEE*, Qiu Tang, Kunzhi Zhu, Weikang Wang, *Graduate Student Member, IEEE*, Yilu Liu, *Fellow, IEEE*, and Wenxuan Yao, *Member, IEEE*

***Abstract*—The synchrophasor data recorded by Phasor Measurement Units (PMUs) plays an increasingly critical role in the regulation and situational awareness of power systems. However, the widely installed PMUs are vulnerable to multiple malicious attacks from cyber hackers during data transmission and storage. To address this problem, a Modified Ensemble Empirical Mode Decomposition (MEEMD) is proposed first to extract the intrinsic mode functions of each Synchrophasor Data Attacks (SDA). The frequency-based adaptive screening criterion embedded in MEEMD is used to eliminate the false intrinsic mode functions. Next, a Multivariate Convolutional Neural Network (MCNN) is proposed to identify multiple SDA by utilizing the extracted intrinsic mode functions and original SDA as input vectors. A fusion block as the main structure of MCNN is also leveraged to increase the diversity of features and compress the model parameters. Integrating MEEMD and MCNN, a framework with automatic feature extraction and multi-source information fusion capability, referred to as Feature Interactive Network (FIN), is proposed to detect multiple SDA. Based on the proposed FIN framework, six types of SDA are explored for the first time using actual synchrophasor data in FNET/Grideye that was collected from different locations in the U.S. Eastern Interconnection. Finally, a large quantity of experiments with different attack strengths are used to evaluate the adaptability and classification performance of the proposed FIN.**

***Index Terms*—Feature interactive network (FIN), multivariate convolutional neural networks (MCNN), synchrophasor data attacks.**

Manuscript received January 27, 2020; revised April 21, 2020 and June 30, 2020; accepted July 25, 2020. Date of publication August 5, 2020; date of current version December 21, 2020. This work was supported in part by the Engineering Research Center Program of the National Science Foundation, DOE through NSF under Award EEC-1041877, in part by the CURENT Industry Partnership Program, in part by the Postgraduate Scientific Research Innovation Project of Hunan Province, and in part by the China Scholarship Council (CSC). Paper no. TSG-00130-2020. *(Corresponding author: Wenxuan Yao.)*

Wei Qiu is with the College of Electrical and Information Engineering, Hunan University, Changsha 410082, China, and also with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996 USA (e-mail: qiuwei@hnu.edu.cn).

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

Weikang Wang is with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996 USA (e-mail: wwang72@vols.utk.edu).

Yilu Liu is 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).

Wenxuan Yao is with the Electrical and Electronics Systems Research Division, Oak Ridge National Laboratory, Oak Ridge, TN 37830 USA (e-mail: yaow1@ornl.gov).

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

Digital Object Identifier 10.1109/TSG.2020.3014311

NOMENCLATURE

Acronyms

1D	One-dimensional
2D	Two-dimensional
CC	Composite Convolution
CNN	Convolutional neural networks
DS	Depthwise separable
EEMD	Ensemble Empirical Mode Decomposition
EI	Eastern Interconnection
FB	Fusion block
FDI	False data injection
FFT	Fast-Fourier Transform
FIN	Feature interactive network
GAP	Global average pooling
IMFs	Intrinsic mode functions
LOF	Local outlier factor
MCNN	Multivariate convolutional neural network
MEEMD	Modified EEMD
NW	Negative weight
PMUs	Phasor measurement units
SC	Standard convolutional
SD	Synchrophasor data
SDA	Synchrophasor data attacks
SEB	Squeeze-and-Excitation block
SVM	Support vector machines
WAMS	Wide area measurement system.

Sets

Ai	The ith type of attack signal
$a(t)$	Combination of IMFs and original SDA
$F(t)$	The IMFs of SDA
K	Total number of SDA categories
M	Empirical data set for selecting N
N	Number of IMFs
$\bar{y}(t)$	Original SDA.

Functions

$I(x)$	Signum function

1949-3053 © 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: UNIVERSITY OF TENNESSEE LIBRARIES. Downloaded on September 20,2024 at 14:41:46 UTC from IEEE Xplore. Restrictions apply.

$\bar{Y}(t)$	FFT frequency spectrum of $\bar{y}(t)$
$f()$	RELU activation function
O_{cr}^{iD}	Output of standard convolutional layer
O_{pr}^{iD}	Output of pooling layer
O_{2pr}^{iD}	Output of negative weight layer
O_{fr}	Output of fusion layer
$S(F)$	Output probability value of softmax.

Variables

b_{cr}^{iD}	Biases in crth iD convolutional layer
d_c^{iD}	Depth of convolution kernel
k_c^{iD}	Size of convolution kernel
l_f^{iD}	Size of filter area
p_s	Output probability of FIN
s_c^{iD}	Stride of convolution kernel
T	Threshold
W	Weighting factor in negative weight
W_{cr}^{iD}	Weights in crth iD convolutional layer
W_{cr}^{iD}	Weights in crth iD convolutional layer
r	Number of convolutional layer
$r_j(t)$	Residual of jth EMD
α	Threshold parameter of T
θ	Parameter in softmax layer.

I. Introduction

A. Background

NOWADAYS, Phasor Measurement Units (PMUs) as one of the most critical elements in wide-area monitoring systems have been widely deployed in the power grid to monitor the voltage and current in terms of amplitude, phase angle and frequency in real time [1]. However, two major attacks, including physical and cyber attacks, increasingly endanger the trustworthiness of the synchrophasor data and inhibits its security against illicit tampering [2]. Meanwhile, the content of the Synchrophasor Data (SD) packet may be maliciously manipulated since the transfer protocol IEEE C37.118 lacks security mechanisms and confidentiality [3]. As a result, not only will the authentication of SD be affected, but the entire system's situational awareness will also be degraded. For example, the frequency would deviate extremely in wide-area damping control when the data spoofing occurs [4].

Essentially, the cyber attacker can inject deceiving data that is difficult to be identified as fake, eventually impairing the normal operation and control system, by providing an inaccurate state estimation. And the system could be induced to produce an erroneous decision and slow down the response speed during power system disturbances [5].

One type of cyber attack referred to as the False Data Injection (FDI) is difficult to be detected especially for the artificially tampered SD [6]. In addition to the difficulties detecting the spoofed data, such cyber attacks can have great consequences economically and politically. More importantly, the FDI attack can occur at different stages of the power system, such as the communication and network stage. It is the variability of this attack method that makes detection more difficult [7].

Apart from the aforementioned effects, the Wide Area Measurement System (WAMS) still faces some cyber security challenges in three aspects, including the device, communication, and control center application [8]. In the device level, the measurement value of the measuring unit device is tampered through interference. The communication channels can be attacked due to the vulnerabilities of the protocols [9]. At the third stage, some power system applications, such as disturbance detection and triangulation [10], can be seriously threatened. Some specific attack behaviors are therefore analyzed considering the severity of FDI attack.

In terms of data spoofing in FDI, the data spoofing attack is stealthy and volatile. In [4], three types of spoofing attacks are developed to explore the impact of attacks on source authentication. The frequency data is attacked by arbitrary PMUs thus confusing authentication information. Meanwhile, two kinds of integrity attacks are proposed to study the response of the grid frequency control system in [11]. The results demonstrate that automatic generation control depends heavily on real-time synchrophasor data. To improve the recognition of multiple Synchrophasor Data Attacks (SDA), an automated attack detection system is urgently required.

B. Related Works

Recently, several methods have been proposed to detect FDI attacks for SD [12]. Generally, these methods can be classified into two categories: anomaly detection and time-spatial signature methods [13].

In the anomaly detection method, it provides a way to detect SDA by observing data distribution. Commonly used outlier detection algorithms include density basis and distance basis methods, such as k-nearest neighbors and Local Outlier Factor (LOF) [14]–[16]. For example, a density basis method named LOF is proposed to detect the FDI and other low-quality SD in [17]. Although LOF has a fast detection speed, the threshold selection of the LOF score will affect the detection result. To address this problem, the symbolic aggregation approximation is introduced to forecast time series SD, which combines different anomaly detection methods [5], [18]. Additionally, the ensemble-based algorithm over PMU data is proposed to detect the noise and missing data attack [1]. However, the ensemble-based algorithm is difficult to identify different SDA due to the high shape and amplitude similarity of SDA to the attack free SD. For example, the replacement attack, part of the data is replaced by SD from other PMUs, which is very close to normal data [7]. In [19], the problematic SD is treated as an anomaly and is cleaned up using the Kalman filter method. One problem of the anomaly detection method is that the tampered SD does not necessarily have a distinguishable density or distance from the original SD. Therefore, effective methods are needed to improve the accuracy from the non-abnormal perspective under multiple attacks.

Since the signature of SDA is difficult to distinguish in the time domain, time-spatial signature methods are used to extract the features. In [20], the Mathematical Morphology (MM) method is used to decompose the frequency measurement data. Then, the two signature features are extracted and fed to the

Authorized licensed use limited to: UNIVERSITY OF TENNESSEE LIBRARIES. Downloaded on September 20,2024 at 14:41:46 UTC from IEEE Xplore. Restrictions apply.

classifier. Analogously, in [21], the Fast-Fourier Transform (FFT) of filtered SD is proposed to classify synchrophasor data from multiple sources. The results of [20], [21] demonstrate that SD collected from different locations contains unique time-spatial signatures, whose integrity can be used as an indicator for attack detection. Nevertheless, the two methods mentioned above require the SD to be filtered, and the filtering effect directly affects the validity of the signatures. To get rid of the filter restrictions, two maximum correlation signatures are formalized. Thus the spoofed SD can be identified using Support Vector Machines (SVM) [22]. However, only three attack modes are considered, making it difficult to apply in complex grid environments. Thereafter, the Bayesian-based approximated filter is used to detect four types of FDI, where the oscillation frequency and damping ratio signatures are extracted from PMUs [23]. This Bayesian prediction's accuracy without prior information is susceptible to outliers.

Some other signature-based methods can also be found in [24], [25]. Specifically, the SVM and k-nearest neighbor are proposed to detect the attack problems [24]. And the covariance of the samples is utilized to identify FDI attack in [25] based on the principal component analysis. The shortcoming of these two methods is that the adaptability is limited due to the manual signature extraction. As discussed previously, less than four types of attacks are verified in [22], [23], which is not sufficient to reflect the diversity of attacks. Hereby, the necessity to develop a method with an automatic feature extraction and intelligent recognition for multiple attack detection arise.

The attack detection is essentially an identification and classification problem via feature extraction. Recently, with the evolutionary combination of Graphical Processing Unit (GPU), the Convolutional Neural Networks (CNN) have been adopted in solving various power system problems including power quality diagnosis [26], [27], power system measurement and control [28], and cyber security detection [29], [30]. It demonstrates that the CNN can efficiently extract features for signal identification. Thus, it is logical to exploit this ability for multi SDA detection, which contains complex spatio-temporal characteristics. However, the effectiveness of CNN is limited by a large number of parameters due to the large multitude of features to be extracted. To solve this, a vector convolutional deep learning method is used to classify the denial of service attack in [31] by compressing the feature vector. Unfortunately, the CNN still suffers from the limited input information because generally only one-dimensional (1D) or two-dimensional (2D) data are used, resulting in reduced performance. Hence, a more efficient method is required to detect the SDA.

C. Contribution

To further tackle the challenges of CNN, a novel signature-basis method is proposed to detect the multiple SDA. The contributions of this paper are listed as follows:

1) To improve the ability of signature extraction, a Modified Ensemble Empirical Mode Decomposition (MEEMD) is proposed to extract Intrinsic Mode Functions (IMFs) of multiple SDA. The number of IMFs is automatically selected using the threshold setting method. The false IMFs can be avoided under different types of SDA.
2) To reduce the impact of manual features, a Multivariate CNN (MCNN) is proposed to fuse multiple input information sources, including the original SDA and extracted IMFs by MEEMD. Particularly, a Fusion Block (FB) is presented to fuse different dimension features with fewer parameters, while the Negative Weight (NW) and Global Average Pooling (GAP) methods are used to reduce the number of parameters.
3) Furthermore, a multiple SDA classification framework, named Feature Interactive Network (FIN), is proposed based on the MEEMD and MCNN. The signatures are extracted automatically without the requirement of manual design. Moreover, the sensitivity of the minimum attack range can be reached up to $1e^{-5}$ p.u.
4) Using the actual SD set in U.S. Eastern Interconnection (EI), a variety of experiments are conducted to verify the validity of the proposed framework. Particularly, six types of SDA comprising scaling attack, ramp attack, pulse attack, random noise attack, replacement attack, data loss attack, are used for performance evaluation. The detection results indicate that the proposed framework has greater accuracy and fewer parameters compared with the advanced machine learning methods.

The remainder of the paper is organized as follows. SDA numerical models are presented in Section II. Then the extraction of attack signatures using modified EEMD is introduced in Section III. Section IV presents the MCNN with the proposed fusion block. The proposed FIN consisting of MEEMD and MCNN is introduced in Section V for SDA detection. Thereafter, various attack experiments are conducted in Section VI for performance assessment. Finally, the conclusion is drawn in Section VII.

TABLE I
ATTACK NUMERICAL MODELS OF DIFFERENT ATTACK METHODS

SD attack types	Attack numerical models
A1: Normal SD	$\bar{y}(t) = y(t)$
A2: Scaling attack	$\bar{y}(t) = y(t)(1 \pm \lambda_2(u(t-t_1) - u(t-t_2)))$ $0 < t_2 - t_1 < L_t$
A3: Ramp attack	$\bar{y}(t) = y(t) \pm \lambda_3 t(u(t-t_1) - u(t-t_2)))$ $0 < t_2 - t_1 < L_t$
A4: Pulse attack	$\bar{y}(t) = y(t) \pm \lambda_4 \delta(t_n)$ $t_n \in t, n = 1, 2, ..., 20$
A5: Random noise attack	$\bar{y}(t) = y(t) + G(u(t-t_1) - u(t-t_2))$ $0 < t_2 - t_1 < L_t$
A6: Replacement attack	$\bar{y}(t) = y(t)(1 + u(t-t_2) - u(t-t_1)) + y_i(t)(u(t-t_1) - u(t-t_2))$ $0 < t_2 - t_1 < L_t, t_1 \geq 0, i = 0, 1, ..., m$
A7: Data loss attack	$\bar{y}(t) = y(t)(1 + u(t-t_2) - u(t-t_1)) + f_0(u(t-t_1) - u(t-t_2))$ $0 < t_2 - t_1 < L_t, t_1 \geq 0, f_0 = 60Hz$

The t_1 and t_2 are the start and end time of the attack respectively. The $u(t)$ is the heaviside step function. The L_t is the sampling time of each SD sample. The G represents the uniform noise.

II. SDA NUMERICAL MODELS

Apparently, each individual data tampering method has its characteristic. In this paper, six types of common SDAs are considered according to [13], [23]. These SDAs consist of

Authorized licensed use limited to: UNIVERSITY OF TENNESSEE LIBRARIES. Downloaded on September 20,2024 at 14:41:46 UTC from IEEE Xplore. Restrictions apply.

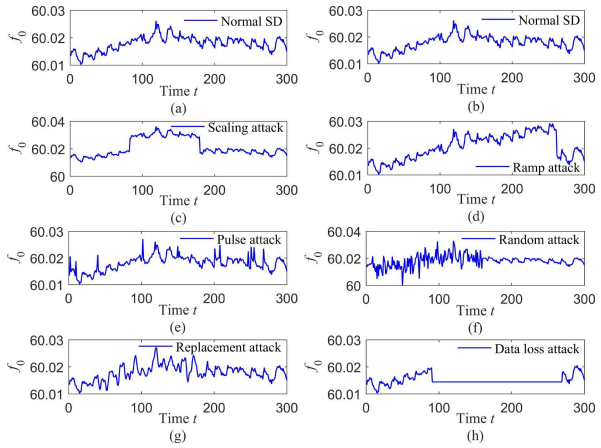


Fig. 1. Six types of SD attacks. (a) and (b) The same normal SD. (c) Scaling attack. (d) Ramp attack. (e) Pulse attack. (f) Random noise attack. (g) Replacement attack. (h) Data loss attack.

scaling attack (A2), ramp attack (A3), pulse attack (A4), random noise attack (A5), replacement attack (A6), and data loss attack (A7). The normal SD is labeled as A1. Denoting the measured normal and attacked synchrophasor data as $y(t)$ and $\bar{y}(t)$, respectively, where t is the time index, the numerical models of six types of SDAs are summarized in Table I.

The strengths of SDA determine whether the attack is easy to identify. The strength means the maximum attack magnitude relative to the normal measurements. Obviously, attack detection methods should be able to deal with attacks at different strengths. To ensure the effectiveness of the attack, the detection performance under a small strength is preferentially explored. For example, to illustrate different types of attacks, the frequency measurement of synchrophasor is analyzed as the case study. Frequency data is stochastic, which is beneficial to verify the effectiveness of the method. Meanwhile, to realize the attack detection of different measurement data in multiple locations, the frequency, phase, and amplitude can be trained together. The dimensions of each dataset need to be the same so that the input vector of FIN can be matched when the data are trained together. Considering actual frequency measurement error can reach 5 mHz due to the impact of the hardware noise and the quantization limitation in PMUs [32], the minimum strength of each attack is set to 5 mHz. Consequently, the strength parameters λ_2 and $\lambda_3 t$ in Table I are constrained to $[0.000084, +\infty]$ referring to [13]. The G is the uniform noise, of which the range of boundary values is $[0.002, +\infty]$.

An example of six types of SDA is shown in Fig. 1. It shows that replacement and ramp attacks have a high similarity with normal SD, which results in those two kinds of attacks being difficult to be distinguished. Meanwhile, the start time and ending time are different for scaling attack and data loss attack, thus resulting in different attack strengths. Therefore, an effective method that is able to distinguish multiple attacks with different characteristics is needed.

III. Modified EEMD in FIN

To distinguish attack signals, the characteristics of the SDA need to be extracted first. Intuitively, the Empirical Mode Decomposition (EMD) is developed to decompose the signal into multiple IMF components, and each IMF contains specific frequency intervals [33]. It is particularly suitable for non-stationary signals analysis. However, the decomposition results of EMD are easily disturbed, resulting in decomposition biases. Thus, an EMD integration form called Ensemble Empirical Mode Decomposition (EEMD) is performed to solve the mode mixing. The primary principle of EEMD is to obtain IMFs by injecting white noise and integrating multiple sub-EMDs [34]. Meanwhile, the time of attack, e.g., jump position can also be strengthened and increased. However, the result of EEMD is prone to generate false components when a fixed number of IMFs is selected. Therefore, the MEEMD is proposed to dynamically select the number of IMFs in FIN.

A. Proposed MEEMD

As the first step of FIN, MEEMD uses the frequency-based adaptive screening criterion to optimize modal aliasing [33]. Before calculating the EEMD, the frequency-based adaptive screening strategy is adopted.

Specifically, a threshold based on FFT and EMD is used to optimize the number of IMFs parameter N. The frequency components of each IMF are expected to be significant enough to increase decomposition efficiency. To determine the frequency component of SDA signal $\bar{y}(t)$, the FFT is used to calculate frequency spectrum $\bar{Y}(t)$. Then, a threshold T is obtained by extracting the maximum and minimum amplitude of $\bar{Y}(t)$. By adopting this spectrum threshold limit, the spectrum of each IMF component will be greater than T. The threshold can be obtained as

$$T = \bar{Y}(t)_{min} + \alpha\left(\bar{Y}(t)_{max} - \bar{Y}(t)_{min}\right) \tag{1}$$

where the $\bar{Y}(t)_{max}$ and $\bar{Y}(t)_{min}$ denote the maximum and minimum amplitude of $\bar{Y}(t)$ respectively, and the $\alpha = 0.3$ is the threshold parameter. The T is used to screen IMFs using frequency peaks of $\bar{Y}(t)_{min}$.

To select a suitable number of IMFs, the EMD of $\bar{y}(t)$ under different N is first obtained. The IMFs of EMD can be expressed as $1th, 2th, \ldots,$ and Nth, where the $1th$ IMF is the high frequency component. The Nth IMF is the low frequency residual component, which is also an attack trend feature.

A larger N value indicates that there are more false components under the same decomposition principle. For example, under two different N (set to N^1 and N^2), and $N^1 < N^2$, the N^1, $N^1 + 1$, $N^2 th$ IMFs components of N^2 are derived from the $N^1 th$ residual term of N^1. Therefore, the false component is closer to the residual term (Nth IMF) as N increases. And the corresponding spectrum amplitudes of IMFs are calculated in reverse order starting from the $(N-1)th$ IMF to $(N-2)th$ IMF, of which can be expressed as $Y_{IMF_{N-i}}$. The i is set to 1, 2 in order to strike a balance between efficiency and accuracy. To reduce the impact of spectrum aliasing, a frequency-based adaptive screening criterion is used to select N from empirical data set $M = \{4, 5, 6, 7\}$, which can be defined as

$$N = I\left(\sum_{i=1}^{2} sign\left[\left(Y_{IMF_{N-i}}\right)_{max} - T\right)\right]\right)$$

Authorized licensed use limited to: UNIVERSITY OF TENNESSEE LIBRARIES. Downloaded on September 20,2024 at 14:41:46 UTC from IEEE Xplore. Restrictions apply.

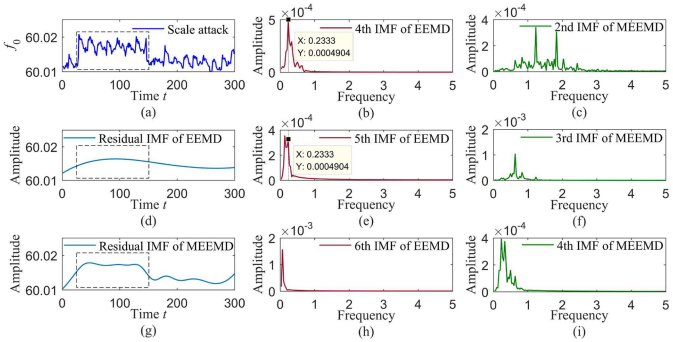


Fig. 2. The performance comparsion of EEMD and MEEMD. The dotted box indicates the location where the attack occurred. (a) Scale SDA. (d), (g) are the residual IMF of EEMD and MEEMD respectively. (b), (e) and (h) are the FFT of $4th$, $5th$, $6th$ IMF in EEMD, respectively. (c), (f) and (i) are the FFT of $2th$, $3th$, $4th$ IMF in MEEMD, respectively.

$$I(x) = Index(x \geq 0)_M \tag{2}$$

where $sign()$ is the signum function, the $I(x)$ indicates that the index of the data set M when x satisfies not less than 0. To reduce the search time, the parameter N is searched from 7 to 4 with step 1.

After selecting N, a total of N_I EMDs are calculated and integrated, where N_I is the number of EMD in MEEMD. Accordingly, the MEEMD of SDA consists of the following four parts:

1) Frequency-based adaptive screening criterion: the threshold T is first calculated based on the FFT of SDA. Combining with T and equation (2), the number of IMFs parameter N is then optimally selected by searching from M. N can be determined when the equation (2) is satisfied for both $(N-1)th$ and $(N-2)th$ IMFs.
2) Noise superposition: the zero-mean Gaussian white noise is first added to $\bar{y}(t)$, where the magnitude is set to 0.2.
3) Perform EMD: MEEMD performs N_I times of EMD for each $\bar{y}(t)$.
4) Data average: the result can be obtained by averaging the N_I EMD to get the final N IMFs.

Thereafter, the SDA $\bar{y}(t)$ can be decomposed into the sum of multiple IMFs and residuals as follows

$$\bar{y}(t) = \sum_{i=1}^{N}\left[\sum_{j=1}^{N_I}\left(IMF_{ij}(t) + r_j(t)\right)\right] \tag{3}$$

where the $IMF_{ij}(t)$ denotes the ith IMF of $\bar{y}(t)$ in the jth EMD and, the $r_j(t)$ denotes the residual of jth EMD.

Hereby, different IMFs of SDA, denoted as $F(t) = \sum_{j=1}^{N_I} IMF_{ij}(t) + r_j(t)$, can then be extracted.

B. Comparison of EEMD and Proposed MEEMD

To verify the actual decomposition effect of the MEEMD, the residual results and FFT components of IMFs are shown. As demonstrated in Fig. 2, the number of IMFs N is set to 7 in EEMD and optimized to 5 in MEEMD. The last three IMFs are presented because the false components are more likely to appear at low frequencies.

TABLE II
THE RELATIONSHIP BETWEEN α AND THE NUMBER OF IMFS FOR DATA LOSS ATTACK

The α in T	Ratio of IMFs under different N (%)			
	7	6	5	4
0.1	61.53	36.17	2.29	0.01
0.3	61.18	36.45	2.34	0.03
0.5	60.68	36.81	2.46	0.05
0.7	60.08	37.05	2.79	0.08

It can be seen from Fig. 2(d), (g) that the residual IMF of MEEMD is closer to the trend of scale attack, which indicates that the trend feature of the attack is correctly extracted. It is worth mentioning that the normal and attack signal can be distinguished because this trend feature is only one of all the extracted features in FIN. Some other features, such as the attack strength, data sources, and type of noise, can also be used to distinguish the attack and the attack-free data. As shown in Fig. 2(b) and (e), the same frequency components are extracted by EEMD because they contain the same frequency. The frequency component of Fig. 2(h) does not overlap, but the frequency peaks are still very close to (b) and (e). Conversely, it is observed from Fig. 2(c), (f) and (i) that the location of frequency spike points are different from each other, indicating that IMFs of MEEMD do not contain false components. Therefore, it can be concluded that the attack trend items are extracted and some of false components are avoided.

To show the sensitivity relationship between the parameter α and the number of IMFs, the IMFs of A7 are counted under different α as listed in Table II. It illustrates that the parameter α determines the number of IMFs. The 6 and 7 are selected as the number of IMFs for more than 95% of cases.

Furthermore, to show the statistical characteristics of different EEMD and MEEMD, two statistical indicators are calculated at different number of N including the correlation and kurtosis [35]. A larger correlation and kurtosis show a better decomposition result. The performances with two statistical indicators under different N and types of attack methods are shown in Fig. 3 and 4. The similar correlation and kurtosis are obtained in Fig. 3(a) and 4(a) because the N is adaptively selected for MEEMD. In Fig. 3 and 4, it demonstrates that all types of attack methods obtain higher correlation and kurtosis value especially when $N < 6$, which indicates that the MEEMD performs better. Meanwhile, EEMD and MEEMD have similar statistical characteristics when the N is larger than 6. The results show that the MEEMD has better statistical characteristics because it can reduce modal aliasing by finding a more suitable N.

Next, a multivariate CNN based classifier is used to identify and detect multiple SDA based on the extracted IMFs $F(t)$.

IV. MULTIVARIATE CNN IN FIN

A. Proposed Fusion Block

As the second step of FIN, the features of SDA can be automatically identified using the proposed MCNN by combining the extracted IMFs. In MCNN, both the IMFs $F(t)$ (2D)

Authorized licensed use limited to: UNIVERSITY OF TENNESSEE LIBRARIES. Downloaded on September 20,2024 at 14:41:46 UTC from IEEE Xplore. Restrictions apply.

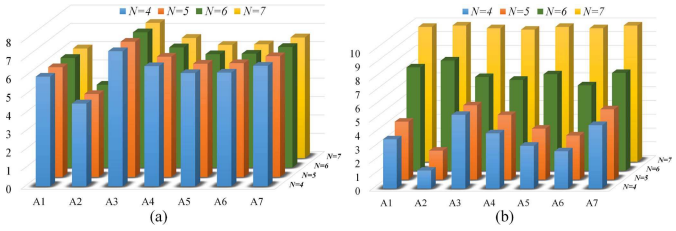


Fig. 3. The correlation between the IMFs and original SD for MEEMD and EEMD methods. (a) MEEMD (b) EEMD.

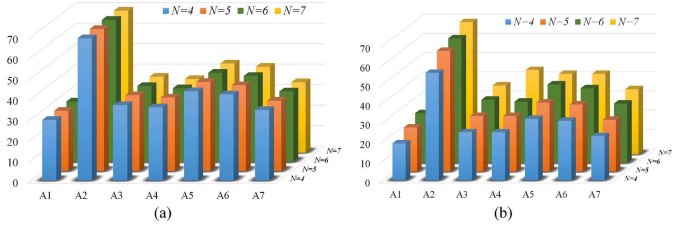


Fig. 4. The kurtosis of IMFs for MEEMD and EEMD methods. (a) MEEMD (b) EEMD.

and original SDA $\bar{y}(t)$ (1D) are used as the inputs. Compared with the traditional CNN methods, the motivation to combine the 1D and 2D feature source is to obtain more diverse and representative because the input of FB is multi-source.

To fuse the 1D and 2D data, a Fusion Block is proposed to improve the diversity of SDA detection in FIN. Two types of convolution kernels, namely 1D and 2D kernels, together form a complete FB from the different dimensions of input. It means that two types of features are extracted. To make full use of the different input source information, the FB is used to simultaneously process two types of data.

The structure of the proposed FB is depicted in Fig. 5. The FB contains two inputs and two outputs. The 1D convolution branch can be used to stack multiple FBs.

Denoting the input data of FB as $a(t) = \{F(t), \bar{y}(t)\}$, the output of Standard Convolutional (SC) layer is calculated as

$$O_{cr}^{iD} = f\left(W_{cr}^{iD} * a(t) + b_{cr}^{iD}\right), \quad i = 1, 2 \tag{4}$$

where the W_{cr}^{iD} and b_{cr}^{iD} are the weights and the biases in the crth convolutional layer for the iD convolution, $r = 1, 2, \ldots, n$ is the number of convolutional layer, the symbol * represents convolution, and $f()$ is the activation function. Meanwhile, the Rectified Linear Unit (RELU) function, where only the positive portion of the input is retained, is selected as the activation function so that the gradient attenuation can be mitigated. The RELU has low computational complexity and can speed up the SDA feature extraction process. The performance and output size of O_{cr}^{iD} are determined by three parameters: the convolution kernel size $k_c^{iD}, i = 1, 2$, convolution depth d_c^{iD} and convolution stride s_c^{iD}. Here, the stride s_c^{iD} is set to 1 and the zero padding is used to match the output dimensions of the different convolutions.

The diversity of the SDA features is key to enhance the model's learning ability. Unlike standard convolution, the Depthwise Separable (DS) convolution can increase the SDA

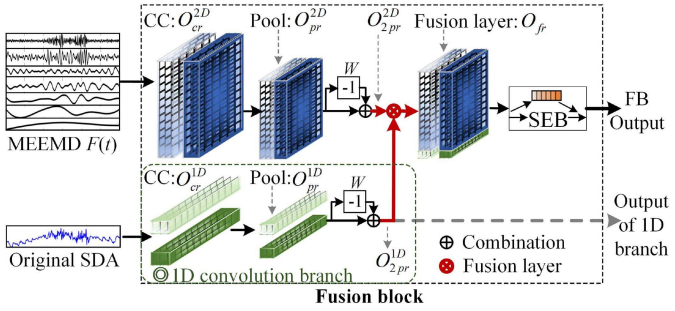


Fig. 5. The structure of the proposed fusion block.

feature space while reducing computation, since each channel can be assigned a kernel with different sizes [36]. In the convolutional layer of FB, a Composite Convolution (CC) is proposed, in which half of the convolutional layers are calculated using DS convolution and the other half uses standard convolution. This means that the $d_c^{iD}/2$ depth of features in CC is obtained from standard convolution and the remaining half is from DS convolution.

Next, a maximum pooling layer is used to reduce the dimensions of the convolution layer features. In this layer, the features of the maximum value are retained, and the smaller values are filtered out. The length of output features becomes $l_p^{iD} = (l_c^{iD} - l_f^{iD})/s_p^{iD} + 1, i = 1, 2$, where l_f^{iD} is the size of filter area, the l_c^{iD} and s_p^{iD} are the output length of O_{cr}^{iD} and stride of pooling layer, respectively. Furthermore, the output of pooling layer can be denoted as O_{pr}^{iD}.

After the pooling layer results are obtained, two additional strategies, including the computational complexity reduction of FB and the multi-input (1D and 2D convolution) fusion, are used to boost the overall performance.

Since the operation of the kernel function is time-consuming, a direct NW method is proposed to increase directly the depth of the feature O_{pr}^{iD}. As shown in Fig. 5, a weighting factor $W = \{-1, -1, \ldots, -1\}$ is multiplied by O_{pr}^{iD}. For a feature set F, the opposite feature set $-F$ can be easily obtained by multiplying -1. Thus more features can be generated and there is no need to perform the convolution operations of the NW method. Then the features are added on the depth axis, which can be expressed as

$$O_{2pr}^{iD} = \left\{O_{pr}^{iD}, W \cdot O_{pr}^{iD}\right\} \tag{5}$$

where the length of W is the same as depth d_c^{iD}. The depth of O_{2pr}^{iD} becomes $2d_c^{iD}$ without the extra learning process. As a result, the proposed FB becomes more lightweight.

Next, the 1D and 2D features are integrated into the new fusion layer. Specifically, the 1D feature is spliced below the 2D feature to form a combined 2D feature. To guarantee a successful merge, the dimension of 1D and 2D features should be matched. For example, if the dimension of the 2D feature O_{pr}^{2D} is (a, b, d), where a and b are the length and width of the feature, the dimension of the 1D feature O_{pr}^{1D} should be $(1, b, d)$ or $(a, 1, d)$. Then the output of fusion layer becomes

$$O_{fr} = \left\{max\left\{0, f\left(W_{cr}^{iD} * a(t) + b_{cr}^{iD}\right)\right\}, \right.$$
$$\left. Wmax\left\{0, f\left(W_{cr}^{iD} * a(t) + b_{cr}^{iD}\right)\right\}\right\}$$

Authorized licensed use limited to: UNIVERSITY OF TENNESSEE LIBRARIES. Downloaded on September 20,2024 at 14:41:46 UTC from IEEE Xplore. Restrictions apply.

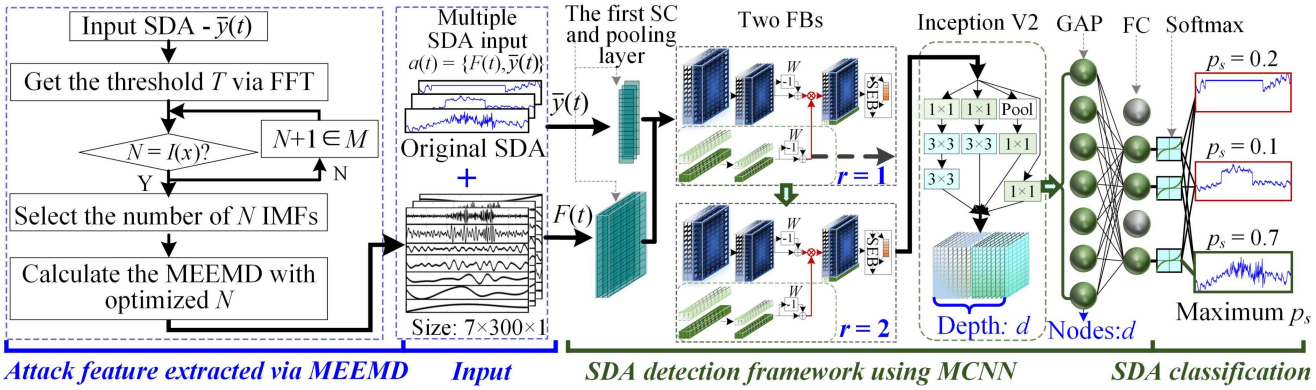


Fig. 6. The SDA detection framework based on FIN.

$$= \left\{ \left\{ O_{pr}^{1D}, W \cdot O_{pr}^{1D} \right\}, \left\{ O_{pr}^{2D}, W \cdot O_{pr}^{2D} \right\} \right\}$$
$$= \left\{ O_{2pr}^{1D}(\bar{y}(t)), O_{2pr}^{2D}(F(t)) \right\} \quad (6)$$

Before getting the results of the FB, it is worth noting that there are still some features in MCNN that may easily become redundant. For example, the distinction between the two types of attack signals is primarily based on the differences between features, rather than on features in common. These common features can be regarded as redundant. To reduce the impact of redundant information, the Squeeze-and-Excitation Block (SEB) can automatically assign a weight to each feature on the depth axis, while adding little computational burden [37]. Therefore, the SEB is further added after the fusion layer to strengthen the difference between features and its representational power.

As can be seen from Eq. (6), the fusion layer fuses the features of $F(t)$ and original SDA $\bar{y}(t)$ into 2D features. The maximization input information of each feature is fully integrated and learned. This fusion method can enrich the feature space because when information of one feature is weak, another feature can make up its deficiency. By stacking multiple FBs, the key features of SDA can be extracted using MCNN.

B. Proposed MCNN

Combined with the aforementioned FB, the complete multivariate CNN framework is established. After stacking multiple FBs, the output features can be obtained.

However, the features of the fusion layer have not been fully integrated and learned in the last FB, i.e., the similarity between 1D and 2D features is not filtered or reinforced. Therefore, an additional convolutional layer is added to the end of the last FB. The inception V2 uses four convolution channels, with the size of each convolution kernel being less than 3×3 [38]. It means that the inception V2 is more efficient in terms of the same computational complexity. To improve the SDA detection accuracy, the inception V2 is selected as the final convolutional layer. In the same way, the weighting factor of NW $W = \{-1, -1, \ldots, -1\}$ is also assigned to the output of the inception V2. Denoting the output of inception block as O_I, the output after the weighting factor W can then be expressed as $O_{2I} = \{O_I, W \cdot O_I\}$.

To achieve the detection of SDA, the extracted SDA features need to be flattened and mapped into the classifier by using a Full-Connected (FC) layer. However, the FC layer tends to introduce a large number of parameters, making the model easy to overfit.

To further reduce the model parameters and the likelihood of overfitting, the GAP layer is introduced to replace the first FC layer. The GAP layer filters each channel for the feature O_{2I} and uses the average value of each channel as an output, thereby greatly reducing the number of parameters [39]. A FC layer with fewer hidden nodes is also added after GAP to adjust the parameters and performance of the model. To reduce overfitting, the dropout layer is then used to randomly discard data of the ratio φ in the FC layer. Finally, the extracted SDA features from the final FC layer is fed to the softmax function. The output of softmax function is set as $f(O_{2I})$. The detected SDA category can be calculated by the following formula

$$p_s(\bar{y}(t) = K | \theta, f(O_{2I})) = \frac{exp^{\theta_{jf}\left(O_{2I}^{j}\right)}}{\sum_{k=1}^{K} exp^{\theta_{kf}(O_{2I}^{k})}} \quad (7)$$

where $\theta_j, \theta_k \in \theta$ are the parameters of softmax function for each class of SDA, and $j, k = 1, 2, \ldots, K, K = 7$ is the total number of SDA categories. The position at the maximum probability value $max(p_s())$ is the attack category identified by the model.

V. SDA Detection Framework Based on FIN

By integrating the MEEMD and MCNN proposed above, a FIN framework with two FBs is proposed in this Section. The FIN framework is shown in Fig. 6. It shows that a standard convolution layer and pooling layer is first used to control the input dimension, ensuring the data can be matched and fused in FB.

As can be seen, the FIN framework of SDA detection can be divided into two parts:

1) Attack features extracted using MEEMD: The IMFs of multiple SDA $\bar{y}(t)$ are first extracted to obtain the $F(t)$ based on the MEEMD. Then both the original SDA and extracted IMFs are combined to get the $a(t)$. The size of each $F(t)$ is 7×300, where some null values are padded with 0 when N is less than 7.

Authorized licensed use limited to: UNIVERSITY OF TENNESSEE LIBRARIES. Downloaded on September 20,2024 at 14:41:46 UTC from IEEE Xplore. Restrictions apply.

2) Automatic SDA detection: A FB is designed to fuse different source information, including $\bar{y}(t)$ and $F(t)$. Specifically, the MCNN, a lightweight network with multiple inputs, is built to identify attack signals.

This FIN is dedicated to detect the attacks before any real power event occurs caused by the FDI attack. Thus the vicious influence will be blocked if the state of program instructions in the power system have changed when the attack just started. According to the FIN results, economic losses will be reduced through real-time detection and fast response. Here, take the generator speed control as an example [4]. The power system controller first needs to stop responding to the current measurement value once an attack is detected. After that, this control state can be restored to the previous control state to prevent deterioration. In this scenario, the generator speed control can resume control once the detection result of the normal signal is given by FIN.

VI. Experiment and Analysis

To verify the effectiveness of the FIN method, various experiments have been conducted under different attack types and strengths in Table I. The actual synchrophasor data from ten locations (L1-L10) in EI of FNET/Grideye [40] was selected, as depicted in Fig. 7. In this Section, the data from locations L1-L9 were used as the normal SD. According to the numerical attack model, the attack A2-A5 and A7 and corresponding labels can be generated based on the normal SD. For the replacement attack A6, the DS from L10 is used to attack the data from other locations. This data from different locations are processed separately in the testing process. Meanwhile, the data of these locations can be detected together through sequential detection. It is worth mentioning that when the grid signal and the attack signal are very similar, the synchronization features of data from multiple locations can be combined to detect SDA comprehensively.

For each type of attack signal, 90468 samples are generated, the length of each being 300 (corresponds to 30 seconds). In the experiment, 40% of the data is used for training, 30% is used for verification and the rest is used for testing. During the training process of MCNN, the Adam optimizer is used to optimize the cross entropy loss function. In total, 30 epochs are set in the Keras for the training of MCNN. To achieve online detection, synchrophasor data in different locations need to be intercepted by a sliding window method. The length of this window is half a minute, and the distance between each window can be set from 10 to 100 (1 to 10 seconds) to satisfy real-time requirements.

A. Parameter Selection for MEEMD and MCNN

The parameter α determines the number of IMFs N. To select a suitable α, the grid search method is used. Four α values are tested with step 0.2. The result is listed in Table III. It can be seen that when $\alpha = 0.1$, the FIN obtains the lowest accuracy. It is because the setting of N is nearly invalid at this time. However, the accuracy gradually decreases when increases. The number of decompositions will be affected when $\alpha > 0.5$. As a compromise, $\alpha = 0.3$ is finally selected.

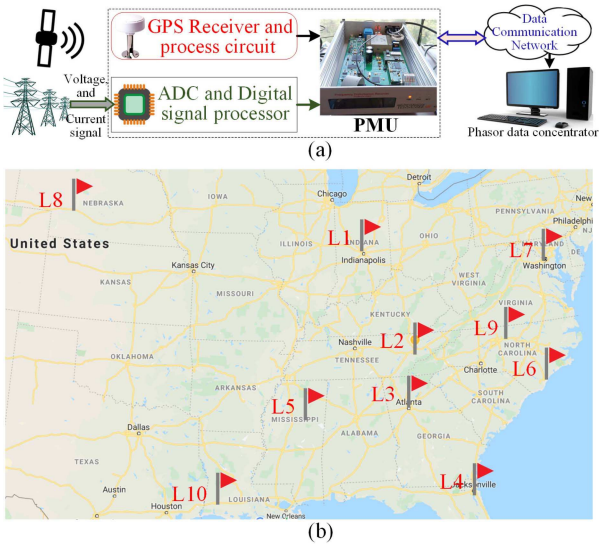


Fig. 7. The PMU signal acquisition schematic and locations in EI. (a) Signal acquisition schematic. (b) The actual SD from ten locations of FNET/Grideye.

TABLE III
The Performance of FIN Under Different α

α	0.1	0.3	0.5	0.8
Accuracy (%)	91.88	93.14	92.30	92.12

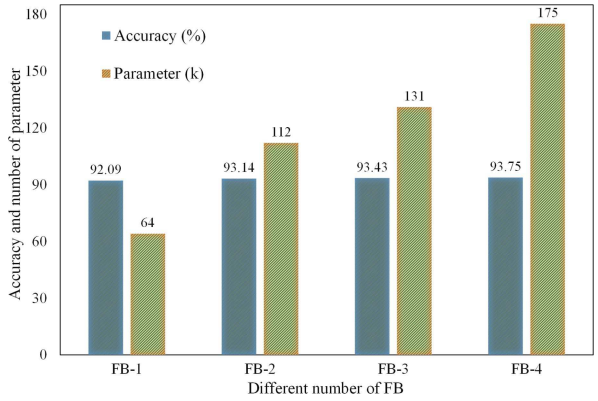


Fig. 8. Performance under different number of FB. The FB-i denotes the number of stacked FB is i. The unit k means thousand.

Additionally, the parameters of MCNN have a great impact on its performance. Particularly, the number of FB determines the parameter capacity and performance of the FIN simultaneously. Therefore, the performance of MCNN under different FB numbers is first explored. In this experiment, the depth d in Inception V2, the nodes in the FC layer, and the dropout parameter are set with the same value for a fair comparison. The SDA detection result under different numbers of FB is illustrated in Fig. 8, where the amplitude of the attack A2-A5 is uniformly set to 5 mHz.

As the number of FB layers increases, it clearly shows that the number of parameters gradually increases for MCNN. Meanwhile, the number of model parameters do not exceed 200 thousands even if there are four FBs. It is observed that the rate of accuracy increases slowly when the number of FB

Authorized licensed use limited to: UNIVERSITY OF TENNESSEE LIBRARIES. Downloaded on September 20,2024 at 14:41:46 UTC from IEEE Xplore. Restrictions apply.

TABLE IV
THE OPTIMIZED PARAMETERS IN MCNN

Types	Parameters in different layers				
	1st	FB (r=1)	FB (r=2)	GAP	FC
1D kernel	13	$k_c^{1D}=13$	$k_c^{1D}=13$	-	-
2D kernel	15×9	$k_c^{2D}=15\times 9$	$k_c^{2D}=15\times 9$	-	-
1D depth	8	$d_c^{1D}=16$	$d_c^{1D}=64$	-	-
2D depth	8	$d_c^{2D}=16$	$d_c^{2D}=64$	-	-
1D Pool	2	$l_f^{1D}=2$	$l_f^{1D}=3$	-	-
2D Pool	(1, 2)	$l_f^{2D}=(2,2)$	$l_f^{2D}=(2,3)$	-	-
Nodes	-	-	-	256	100

TABLE V
PERFORMANCE COMPARISON WITH DIFFERENT FIN STRUCTURES

Models	Accuracy (%)	Number of parameter	Test time (ms)
FIN-no SEB	91.41	111.4 k	0.308
FIN-no Inception V2	90.29	62.7 k	0.264
FIN-no GAP	93.25	752 k	0.305
FIN	93.14	112 k	0.310

is larger than 2. This means that increasing the number of FB does not significantly improve the accuracy when $r > 2$. Thus, considering the trade-off between the complexity of the model and classification accuracy, the number of FB is set to 2.

After the number of FB is determined, the hyperas is called to select the optimized parameters [41]. For discrete variables, such as kernel size $k_c^{iD}, i = 1, 2$, and convolution depth d_c^{iD}, the hyperas selects parameters by searching in a specified dataset. For continuous variables, the hyperas searches for the optimized value in the uniform distribution. For example, the ratio φ parameter of the dropout layer can be searched in the *Uniform*$(0.1, 0.5)$, where the 0.1 and 0.5 are the lower and upper bounds respectively.

Using the optimization method, the following parameters are finally adopted as listed in Table IV. Additionally, the dropout parameter ratio is set to $\varphi = 0.3$.

Based on optimized parameters, to verify the effectiveness of SEB, Inception V2 and GAP, the accuracy of FIN is shown in Table V when these components are not included respectively. The input of these four models are the same. The test time is the running time of each sample for the FIN structure part. It can be seen that the parameters and test time of FIN without SEB is similar to FIN. However, the accuracy of FIN is higher, indicating that the SEB contributes to the accuracy of SDA detection. Meanwhile, it shows that the FIN without Inception V2 has the lowest accuracy and minimal parameters. The accuracy of the FIN without GAP is higher than 93%. However, the number of parameters of FIN without GAP is 7 times than FIN. Overall, it means that the Inception V2 can improve the accuracy while the GAP helps to reduce the model parameters.

B. Performance Under Different Attack Strengths and Time

The attack strength determines the sensitivity of SDA detection. To verify the validity of the FIN, the raw methods including EEMD and CNN, are used to compare against one another under different attack strengths. According to the range of the attack strengths, the strength conditions are set to 5 mHz, 10 mHz and 20 mHz respectively. For example, the λ_2 and $\lambda_3 t$ in Table I are set to 0.00033 when the attack strength is 20 mHz. In regular EEMD, the number of IMFs is set to $N = 5$ here. For the regular CNN, the number of convolutional layer is set to 4 which is consistent with MCNN. The number of nodes is set to 100 in the FC layer. The other parameters, such as the kernel size and depth, are set with the same values as MCNN to make a fair comparison. It is noted that the original SDA $\bar{y}(t)$ cannot feed into the regular CNN due to the constraint of 2D shape.

TABLE VI
PERFORMANCE COMPARISON UNDER DIFFERENT ATTACK STRENGTHS

Models	Accuracy (%)			Number of parameter	Test time (ms)
	5 mHz	10 mHz	20 mHz		
1DCNN	91.23	96.51	98.92	491 k	**3.85**
EEMD-CNN	90.04	96.64	98.73	2856 k	54.30
MEEMD-CNN	91.63	97.45	98.84	2856 k	57.30
EEMD-MCNN	91.74	97.35	98.85	**112 k**	54.27
FIN	**93.14**	**97.67**	**99.18**	**112 k**	57.27

The results under different attack strengths are listed in Table VI. The input of the EEMD-CNN, MEEMD-CNN, and EEMD-MCNN methods are the 2D data. This means that only 2D features are generated. The input of DCNN is 1D data, which means only 1D features can be generated [27]. The test time refers to the runtime for each test sample. It can be seen that the EEMD-CNN has the lowest accuracy under different attack strengths since the number of parameters is only 62.7 k. The results also show that both MEEMD and MCNN of FIN contribute to the improvement of accuracy in SDA detection. Meanwhile, the accuracy of the combination of 1D and 2D features is higher than the single 1D or 2D features indicating that a higher number of parameters has a richer feature space.

Obviously, the accuracy increases more than 3% when the attack strength is 5 mHz, and the corresponding sensitivity is $1e^{-5}$ p.u. (0.005/60). In contrast, Only 0.5% detection accuracy improvement is achieved in the case of 20 mHz. The reason for this is that the attack strength is high, making it easy to be identified by general CNN. The number of parameters of MCNN is reduced by more than 95% compared with CNN, which facilitates its implementation in a practical field system. Moreover, it can be seen that the real-time SDA detection can be satisfied because each sample can be tested within 57.27 ms. When a higher sampling rate such as 30, 60, and 120 Hz is configured, the strategies such as down-sampling or reducing window length can be applied to reduce the running time.

To verify the time sensitivity to attacks, the accuracy of FIN under different lasting time is listed in Table VII. This lasting time means the duration of the attack. The sign 20/300 denotes the length of the attack is 20 (2 seconds), and 300 (30 seconds) is the total length of each sample. It can be seen that the detection accuracy decreases when the attack's duration is only 20/300. As the lasting time of the attack increases,

Authorized licensed use limited to: UNIVERSITY OF TENNESSEE LIBRARIES. Downloaded on September 20,2024 at 14:41:46 UTC from IEEE Xplore. Restrictions apply.

TABLE VII
PERFORMANCE COMPARISON WITH DIFFERENT LASTING TIME

Lasting time	20/300	50/300	100/300	200/300
Accuracy (%)	89.91	93.97	94.20	93.95

TABLE VIII
PERFORMANCE OF FIN UNDER DIFFERENT ATTACK STRENGTHS

SDA types	Accuracy (%)		
	5 mHz	10 mHz	20 mHz
A1	90.92	97.31	98.94
A2	86.35	95.51	98.16
A3	85.93	95.23	99.17
A4	93.63	97.29	97.55
A5	96.64	99.79	99.96
A6	98.65	99.43	99.77
A7	99.87	99.12	100

TABLE IX
COMPARISON WITH RESULTS OF MACHINE LEARNING METHODS

Models	Structure	Ave. Acc. (%)	Test time (ms)
MEEMD-ANN	2100-1000-300	71.17 $\pm$ 0.216	57.04
MEEMD-SVM	Hinge:0.0051	39.84 $\pm$ 0.173	**57.02**
MEEMD-SAE	2100-600-300	66.39 $\pm$ 0.079	57.03
FIN	Two FBs	**96.66 $\pm$ 0.047**	57.27

Ave. Acc.: Average accuracy, it is calculated under 5, 10 and 20 mHz.

the detection accuracy increases. When the attack's duration is longer than 16%, the proposed method has stable performance.

The detailed performance of different attack strengths are summarized in Table VIII. As can be seen, A2 and A3 can be misidentified easier than other types of attacks. When the attack strength is 5 mHz, the amplitude of scaling and ramp attack are very similar to original SD, resulting in difficulties in extracting the features. Particularly, the minimum accuracy of FIN is 97.55% when the attack strength is 20 mHz. To address the problem of detection accuracy for some attacks, more convolutional layers, channels, and higher reporting rates can be used.

C. Comparison With Machine Learning Methods

To further investigate the performance of MCNN, several conventional machine learning methods, including Artificial Neural Network (ANN), SVM and Stacked Auto-Encoder (SAE), are compared with FIN. The result of MEEMD is straightened to match the input for the ANN and SVM due to the 1D limitation, namely being that the input length is 2100 nodes. For SVM, a linear SVM is selected because it can provide fast calculation taking into account the large dimension of the input vector. Additionally, the 1D convolution layer is used in SAE, then the output of SAE are fed to the softmax classifier. To maintain a reasonable comparison, the number of convolution layers of SAE is optimally selected. The number of parameters for three traditional methods is optimized by using grid search method.

The structure and average detection results are listed in Table IX. From Table IX, it shows that the proposed FIN framework achieves the highest 96.66% detection accuracy and lowest 0.047% uncertainty. As expected, it demonstrates that the accuracy of the traditional methods is not satisfactory although they consume less test time. For example, the average accuracy of SVM and SAE are only 39.84% and 66.39% respectively.

D. Comparison With Recent SDA Detection Methods

In this subsection, the proposed FIN is compared with four recent SDA detection methods. An overview of four methods are as follows:

1) WT-FFT-ANN [21]: The synchrophasor data from different areas are identified in this method. This means that the method has potential attack detection capabilities. This detection method is divided into three steps: the common components of SDA are first removed by wavelet-based method. Then the spectrum features are extracted using FFT. Lastly, the three layers of ANN is used to classify the SDA.
2) HF-MM-RFC [4]: The spatio-temporal features of different SDA are extracted to detect the type of SDA. The detection method contains four steps: in the first two steps, the weighted high pass filter and MM methods are used to decompose SDA signals; in the next two steps, the extracted 62 unique indexes are calculated and then fed to gcForest classifier. It is noted that only the replacement attack is tested in this paper.
3) Density based (DB) method: According to [17], the density or distance basis method can be adopted to detect the anomaly synchrophasor voltage data, where the SDA can be treated as outliers. The A5 and A7 attack methods were used in [17]. The LOF is selected to detected the SDA. The result of LOF is a two-category result, in which all of the attacks in A2-A7 are one class and the A1 is another class.
4) DCNN [27]: In this method, the DCNN is utilized to directly classify different raw power quality disturbances. Importantly, the DCNN contains 1D convolution and belongs to a CNN classifier with strong feature extraction capabilities. Therefore, the SDA is directly fed to a six-layer DCNN to make a reasonable comparison.

The performance comparison of four methods are listed in Table X. Compared with WT-FFT-ANN and HF-MM-RFC, the accuracy of FIN is as high as 93.14% even when the attack strength is 5 mHz. It indicates that the FIN can mine more valuable features for SDA detection than manual feature extraction. Although the WT-FFT-ANN has fewer parameters (5k), it can only achieve 68.04% under 5 mHz attack condition, which indicates that the features of SDA are not effectively extracted by FFT. Meanwhile, the accuracy of DCNN is approximately 2% lower than FIN, but the number of parameters in DCNN is nearly 4 times larger than FIN, demonstrating that the FIN has a better structure and higher accuracy. Once the attack signal is recognized, some corresponding measures can be taken. For example, the generator can maintain the current speed rather than adjusting based on the attack signal.

Authorized licensed use limited to: UNIVERSITY OF TENNESSEE LIBRARIES. Downloaded on September 20,2024 at 14:41:46 UTC from IEEE Xplore. Restrictions apply.

TABLE X
PERFORMANCE COMPARISON WITH RECENT ATTACK METHODS

Models	Accuracy (%)			Number of parameter
	5 mHz	10 mHz	20 mHz	
WT-FFT-ANN	68.04	72.67	78.18	**5 k**
HF-MM-RFC	50.49	52.48	54.07	-
DB (LOF)	67.50	70.63	75.31	-
DCNN	91.23	96.51	98.92	491 k
FIN	**93.14**	**97.67**	**99.18**	112 k

-: it is not reported.

VII. CONCLUSION

In this paper, a feature interactive network based on the MEEMD and MCNN is proposed to automatically detect and classify multiple SDA. The modal aliasing and false IMF component have been suppressed by a frequency-based screening criterion. Based on the extracted IMFs, the negative weight and GAP are introduced to build a lightweight FB. Thus a MCNN with stacked FB is further proposed to fuse multi-source and dimension input information. The experiments under different attack strengths show fewer parameters, greater accuracy, and real-time of the proposed FIN. Moreover, six different types of attack methods are evaluated using the actual synchrophasor data from FNET/Grideye. Various experiments are carried out and the results demonstrate that the accuracy of FIN has achieved 93.14% even when the attack strength is $1e^{-5}$ p.u. Finally, compared with some common machine learning classifiers (ANN, SVM, and SAE) and recent advanced SDA detection methods, the FIN has a more compact structure and higher detection accuracy. Synchrophasor data from more locations will be further tested. After the SDA is detected, the specific response measures of power grids should also be further studied.

REFERENCES

[1] 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.

[2] 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.

[3] 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)*, Jul. 2016, pp. 1–5.

[4] Y. Cui, F. Bai, Y. Liu, P. L. Fuhr, and M. E. Morales-Rodríguez, "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.

[5] S. Basumallik, R. Ma, and S. Eftekharnejad, "Packet-data anomaly detection in PMU-based state estimator using convolutional neural network," *Int. J. Elect. Power Energy Syst.*, vol. 107, pp. 690–702, May 2019.

[6] 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.

[7] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. 47th Annu. Allerton Conf. Commun. Control Comput. (Allerton)*, 2009, pp. 911–918.

[8] A. Sundararajan, T. Khan, and A. Moghadasi, "Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies," *J. Mod. Power Syst. Clean Energy*, vol. 7, pp. 449–467, Dec. 2019.

[9] F. Zhu, A. Youssef, and W. Hamouda, "Detection techniques for data-level spoofing in GPS-based phasor measurement units," in *Proc. Int. Conf. Sel. Topics Mobile Wireless Netw. (MoWNeT)*, 2016, pp. 1–8.

[10] X. Deng, D. Bian, D. Shi, W. Yao, L. Wu, and Y. Liu, "Impact of low data quality on disturbance triangulation application using high-density PMU measurements," *IEEE Access*, vol. 7, pp. 105054–105061, 2019.

[11] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system," in *Proc. IEEE PES Gen. Meeting*, 2010, pp. 1–6.

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

[13] 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.

[14] S. Ramaswamy, R. Rastogi, and K. Shim, "Efficient algorithms for mining outliers from large data sets," *SIGMOD Rec.*, vol. 29, no. 2, pp. 427–438, May 2000.

[15] H. Liu and C. Chen, "Data processing strategies in wind energy forecasting models and applications: A comprehensive review," *Appl. Energy*, vol. 249, pp. 392–408, Sep. 2019.

[16] X. Wang, D. Shi, J. Wang, Z. Yu, and Z. Wang, "Online identification and data recovery for PMU data manipulation attack," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 5889–5898, Nov. 2019.

[17] M. Wu and L. Xie, "Online detection of low-quality synchrophasor measurements: A data-driven approach," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 2817–2827, Jul. 2017.

[18] M. Yue, "Evaluation of a data analytic based anomaly detection method for load forecasting data," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2018, pp. 1–5.

[19] K. D. Jones, A. Pal, and J. S. Thorp, "Methodology for performing synchrophasor data conditioning and validation," *IEEE Trans. Power Syst.*, vol. 30, no. 3, pp. 1121–1130, May 2015.

[20] 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.

[21] 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.

[22] 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)*, Apr. 2016, pp. 1–8.

[23] H. M. Khalid and J. C. Peng, "A Bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2026–2037, Jul. 2016.

[24] 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.

[25] Y. Ding and J. Liu, "Real-time false data injection attack detection in energy Internet using online robust principal component analysis," in *Proc. IEEE Conf. Energy Internet Energy Syst. Integr. (EI2)*, 2017, pp. 1–6.

[26] W. Qiu, Q. Tang, J. Liu, and W. Yao, "An automatic identification framework for complex power quality disturbances based on multifusion convolutional neural network," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3233–3241, May 2020.

[27] 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.

[28] S. Kiranyaz, A. Gastli, L. Ben-Brahim, N. Al-Emadi, and M. Gabbouj, "Real-time fault detection and identification for MMC using 1-D convolutional neural networks," *IEEE Trans. Ind. Electron.*, vol. 66, no. 11, pp. 8760–8771, Nov. 2019.

[29] F. Ullah *et al.*, "Cyber security threats detection in Internet of Things using deep learning approach," *IEEE Access*, vol. 7, pp. 124379–124389, 2019.

[30] W. Qiu, Q. Tang, Y. Wang, L. Zhan, Y. Liu, and W. Yao, "Multi-view convolutional neural network for data spoofing cyber-attack detection in distribution synchrophasors," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 3457–3468, Jul. 2020.

[31] N. G. Bhuvaneswari Amma and S. Subramanian, "VCDeepFL: Vector convolutional deep feature learning approach for identification of known and unknown denial of service attacks," in *Proc. TENCON IEEE Region 10 Conf.*, Oct. 2018, pp. 0640–0645.

Authorized licensed use limited to: UNIVERSITY OF TENNESSEE LIBRARIES. Downloaded on September 20,2024 at 14:41:46 UTC from IEEE Xplore. Restrictions apply.

[32] J. Zhao *et al.*, "Impact of measurement errors on synchrophasor applications," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2017, pp. 1–5.
[33] N. E. Huang *et al.*, "The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis," *Proc. Math. Phys. Eng. Sci.*, vol. 454, no. 1971, pp. 903–995, 1998.
[34] N. Nizam, K. Alam, and M. Hasan, "EEMD domain AR spectral method for mean scatterer spacing estimation of breast tumors from ultrasound backscattered RF data," *IEEE Trans. Ultrason., Ferroelect., Freq. Control*, vol. 64, no. 10, pp. 1487–1500, Oct. 2017.
[35] J. B. Ali, N. Fnaiech, L. Saidi, B. Chebel-Morello, and F. Fnaiech, "Application of empirical mode decomposition and artificial neural network for automatic bearing fault diagnosis based on vibration signals," *Appl. Acoust.*, vol. 89, pp. 16–27, Mar. 2015.
[36] F. Chollet, "Deep learning with separable convolutions," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, 2016, pp. 1251–1258.
[37] J. Hu, L. Shen, and G. Sun, "Squeeze-and-excitation networks," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2018, pp. 1–13.
[38] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, "Rethinking the inception architecture for computer vision," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2016, pp. 1–10.
[39] T.-Y. Hsiao, Y.-C. Chang, H.-H. Chou, and C.-T. Chiu, "Filter-based deep-compression with global average pooling for convolutional networks," *J. Syst. Archit.*, vol. 95, pp. 9–18, May 2019.
[40] 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.
[41] M. Pumperla. (2019). *Hyperas*. [Online]. Available: https://github.com/maxpumperla/hyperas

Wei Qiu (Graduate Student Member, IEEE) 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.

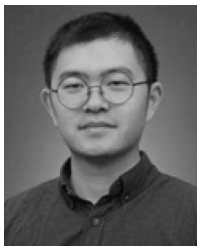
He has been a joint Doctoral student with the University of Tennessee since 2019. His current research interests include power system analysis, cyber-security of synchrophasor, power quality measurement, and reliability analysis of power equipment.

Qiu Tang was born in Hunan, China, in 1970. She received the B.Sc. and M.Sc. degrees in electrical engineering from Hunan University, Changsha, China, in 1992 and 1995, respectively, the M.Sc. degree in electrical engineering from the University of Nottingham, Nottingham, U.K., in 2005, and the Ph.D. degree in electrical engineering from Hunan University in 2010.

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.

Kunzhi Zhu received the B.S. degree in measurement and control technology and instrument from Hunan University, Changsha, China, in 2018, where he is currently pursuing the Ph.D. degree in electrical engineering.

His research interests include signal processing, machine learning, power system analysis, and mechanical fault diagnosis.



Weikang Wang (Graduate Student Member, IEEE) received the B.S. degree in computer science from the School of Control and Computer Engineering, North China Electric Power University in 2016. He is currently pursuing the Ph.D. degree in computer engineering with the University of Tennessee, Knoxville.

His research interests include wide-area monitoring, situation awareness, big data, and machine learning.

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

She is currently the Governor's Chair with the University of Tennessee, Knoxville, and Oak Ridge National Laboratory (ORNL). She is also the Deputy Director of the DOE/NSF-cofunded engineering research center CURENT. Prior to joining UTK/ORNL, she was a Professor with Virginia Tech. She led the effort to create the North American power grid Frequency Monitoring Network (FNET) with Virginia Tech, which is now operated at 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. She is elected as the member of National Academy of Engineering in 2016.

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 applications, embedded system development, power quality diagnosis and big data analysis for the power system.

Authorized licensed use limited to: UNIVERSITY OF TENNESSEE LIBRARIES. Downloaded on September 20,2024 at 14:41:46 UTC from IEEE Xplore. Restrictions apply.