

Cyber-Attack Identification of Synchrophasor Data Via VMD and Multifusion SVM

Wei Qiu, *Member, IEEE*, Kunzhi Zhu, Zhaosheng Teng, Qiu Tang, Wenxuan Yao, *Senior Member, IEEE*, Yuqing Dong, *Student Member, IEEE*, and Yilu Liu, *Fellow, IEEE*

Abstract—A large amount of synchrophasor data in the wide area measurement system (WAMS) needs to be collected and transmitted to the phasor data concentrator, thereby increasing the possibility of being attacked by hackers. The attacked data are therefore hidden into the normal synchrophasor data so that the synchrophasor data based application will be affected. To remedy this problem, an identification framework is proposed to detect the data cyber-attack in WAMS utilizing variational mode decomposition (VMD) and multifusion support vector machine (MSVM). First, VMD is used to transform the attacked data into multiple modal components. Thereafter, a novel MSVM is employed to classify the deterministic features using the proposed linear combined multikernel (LCM). This LCM can fuse multiple types of features, including the time, frequency, and statistical domains of the synchrophasor data. Utilizing the actual data from FNET/GridEye, different experiments are conducted under multiple attack strengths and types. The results demonstrate that the identification framework has higher precision and robustness compared with other conventional classifiers.

Index Terms—Linear combined multikernel (LCM), multifusion support vector machine (MSVM), synchrophasor data, variational mode decomposition (VMD).

I. INTRODUCTION

THE quality of the synchrophasor data collected in the wide area measurement system (WAMS) is critical for

Manuscript received July 22, 2020; revised December 21, 2021; accepted January 12, 2022. Date of publication January 21, 2022; date of current version March 20, 2022. Paper 2020-CSC-0981.R1, presented at the 2020 IEEE Industry Applications Society Annual Meeting, Detroit, MI USA, Oct. 9–14, approved for publication in the IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS by the Codes and Standards Committee of the IEEE Industry Application Society. This work was supported in part by the Current Industry Partnership Program, and in part by the National Natural Science Foundation of China under Grant 52077067. (*Corresponding authors: Kunzhi Zhu; Qiu Tang.*)

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

Kunzhi Zhu, Zhaosheng Teng, Qiu Tang, and Wenxuan Yao are with the College of Electrical and Information Engineering, Hunan University, Changsha 410082, China (e-mail: zhukunzhi@hnu.edu.cn; tengzs@126.com; tangqiu@hnu.edu.cn; wenxuan Yao@hnu.edu.cn).

Yuqing Dong is with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996 USA (e-mail: ydong22@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 Oak Ridge National Laboratory, Oak Ridge, TN 37830 USA (e-mail: liu@utk.edu).

grid situational awareness and disturbance event location [1]. Meanwhile, the synchrophasor measurements from the WAMA provide some insights into power system applications including power system stability, supply and demand response, and market activities [2], [3]. However, the synchrophasor data are vulnerable to cyber-attack, such as false data injection attack (FDIA) and denial of service [4], because the FDIA methods can be achieved secretly due to security holes of IEEE C37.118 [5]. This makes the attack very secret and difficult to be detected. For instance, the attackers can maliciously repeat the measurement from the phasor measurement units (PMUs). Such an attack is not easy to spot and the resulting attack will disturb the time information of the power system [6]. Apart from this, a variety of FDIA methods make it difficult to detect the attack behavior. To enhance the synchrophasor data quality and availability, it is necessary to detect the FDIA from the normal synchrophasor data in the WAMS.

Before responding to any attack, it is essential to accurately identify the type of attack. Generally, cyber-attack identification can be categorized into model-driven and data-driven methods [7]. The model-based detection methods are proposed based on the power system parameters and configuration. The weighted least squares (WLS) is one of the most commonly used model-based methods, which can be used to estimate the system states and topology change caused by FDIA [8]. However, the WLS assumes that the system is operating under steady-state conditions. Therefore, some other novel detection forms are developed from the residual analysis and measurement correlation aspects, such as the multiple robust estimators [9]. As mentioned above, the attackers must have sufficient knowledge to avoid the bad detection algorithm of the target power system in the state estimation-based methods [10].

To reduce dependence on the model and system parameters, different data-driven methods are proposed to learn and distinguish the FDIA. According to the label information of FDIA, the data-driven methods can be classified into two parts including unsupervised and supervised learning methods [11].

The unsupervised methods treat tampered synchrophasor data as anomalies. In [12], five types of attack templates are detected using the developed symbolic aggregation approximation approach. The attacked and original data are separated through observing the maximum errors. However, the occurrence probability of the observation is calculated, which means that the threshold is needed to determine the anomaly. To eliminate this issue, the universal online reinforcement learning (RL) approach

TABLE I
 DEMERITS OF EXISTING FRAMEWORKS

Literature	Methods	Application	Demerits
[20]	Dynamic Symbolic Filtering + Bayesian Networks	Scalable anomaly detection	Use simulated data but not measured data, limited portability
[21]	A detection model and state forecasting method	Data injection detection	
[22]	A DBN-based detection method	False data injection detection	
[23]	Discrete wavelet transformation (DWT)+Back Propagation (BP) net	Source location identification	Use single feature, limited robustness
[24]	Stacked autoencoder based method	SCADA attacks detection	Consider fewer types of attacks
[25]	A nonlinear auto-regressive exogenous model (NARX) neural network	False data injection in DC Microgrids	
[26]	Correlation coefficient + SVM	Spoofed data injection detection	
[27]	Ensemble Empirical Mode Decomposition (EEMD)+FFT+BP	Data authentication	Expensive computing cost
[28]	Restricted Boltzmann Machine	Anomaly network intrusion	

is proposed for cyber-attack detection [13]. The model-free RL is universal for FDIA because it does not need the attack model. Nevertheless, this method is not only complicated, but also difficult to deploy due to a large amount of computing required.

To address the shortcomings of unsupervised learning methods, many supervised learning approaches are designed by learning deterministic information from the synchrophasor data. For example, artificial neural networks (ANN) is used to identify the event of the cyber-attack in the compromised meters [14]. The electrical theft, by tampering with billing alterations, can be detected using the decision tree (DT) and support vector machine (SVM) [15]. And different aspects of raw data are learned by the hidden Markov models and ANN in the supervisory control and data acquisition system [16], the results show 80% performance based on the time feature extraction. However, the ANN and DT can generate overcomplex nodes and trees, resulting in decreased performance in testing data. To overcome this challenge, some advanced methods such as convolutional neural networks [17] are used to automatically extract the features of attack signals. For example, combing with the convolutional neural network and long short-term memory networks, the novel framework is proposed to extract the spatial-temporal correlations [18]. The convolution neural network is also developed for cyber-attack detection in industrial control systems [19]. Due to the diversity of FDIA methods, the robust performance of these networks is limited by the single input information.

To explore the research gap in cyber attack detection, some typical deficiencies of existing frameworks are summarized in Table I. As listed in Table I, some studies use simulation data (based on IEEE 30, 57, 118 bus systems, etc.), which leads to limited portability [20]–[22]. Besides, studies [23] and [24] only consider a single feature or fewer types of cyber attacks. The model with fewer features can consume less calculation time. However, the single feature will lead to insufficient detection results due to less information. Fewer types of attacks will also lead to limited robustness and a decrease in the applicability of the method. Additionally, some methods may consume more calculation time [27], [28], which restricted the applications in some scenarios with real-time requirements.

To further improve the recognition accuracy of FDIA for synchrophasor data in scale power systems, an adaptable model

that can be applied to multiple types of cyber attacks is required. Combined with the advantages of strong feature extraction capabilities of data-driven methods, a novel data-driven framework is proposed. This article is an extension of the IAS conference paper in [29], and our contributions are summarized as follows.

- 1) To identify multiple FDIAs from different aspects, the variational mode decomposition (VMD) is utilized to decompose the attacked synchrophasor data. And four features are designed from the statistics, time, and frequency domains to enhance the feature dimension.
- 2) To improve the recognition accuracy, a multifusion SVM (MSVM) is proposed to fuse various attack features through the linear combined multiple kernels. Typically, MSVM adjusts the combination of deterministic features that facilitate the fusion of multisource information.
- 3) A synchrophasor data based FDIA identification framework VMD-MSVM is proposed based on the VMD and MSVM. Extensive experiments using the actual synchrophasor data are carried out to verify the proposed framework. Experimental results show that this framework is effective for different attack detection even compared with some advanced methods.

The remainder of this article is organized as follows: In Section II, the VMD and definition of extracted features are presented. Then, the proposed MSVM method is described to detect the cyber-attack in Section III. Different experiments are conducted in Section IV. Finally, the experiments are presented and Section V concludes this article.

II. CYBER-ATTACK FEATURE EXTRACTION BASED ON VMD

A. Principle of VMD

VMD is a new multiresolution technology for adaptive and nonrecursive signal decomposition, which is suitable for analyzing nonlinear and nonstationary signals [30]. Compared with empirical mode decomposition (EMD), VMD has strict mathematical theory support. Particularly, modal aliasing can be avoided. Given the shortcomings of the EMD method, the mode aliasing of EMD is also solved by the EEMD [31]. However, the computational complexity of EEMD is also increased since multiple EMD calculations are required. Therefore, VMD is selected

as the feature extraction method for the attacked synchrophasor data.

For the attacked synchrophasor data $f(t)$, the VMD can automatically decompose signal $f(t)$ into multiple intrinsic mode functions (IMFs) with sparse characteristics and limited bandwidth. The sum of all the decomposed IMFs can restore $f(t)$. Specifically, the VMD optimizes the following constraints to generate IMFs, which can be expressed as:

$$\begin{cases} \min_{\{u_n\}, \{\omega_n\}} \left\{ \sum_{n=1}^N \left\| \partial_t \left[\left(\delta(t) + \frac{j}{\pi t} \right) * u_n(t) \right] e^{-j\omega_n t} \right\|_2^2 \right\} \\ \text{s.t. } \sum_{n=1}^N u_n(t) = f(t) \end{cases} \quad (1)$$

where N is the number of decomposed IMFs, $\delta(t)$ is the Dirac delta function, $u_n(t) = \{u_1(t), u_2(t), \dots, u_N(t)\}$ are shorthand notations for the set of all IMFs, $\omega_n = \{\omega_1, \omega_2, \dots, \omega_N\}$ are shorthand notations for the center frequency of $u_n(t)$.

To calculate $u_n(t)$, the amplitude–modulation–frequency–modulation signals can be used as

$$u_n(t) = A_n(t) \cos(\Phi_n(t)) \quad (2)$$

where $A_n(t) \geq 0$ is the envelope of $u_n(t)$, $\Phi_n(t)$ is the phase of $u_n(t)$. For each mode $u_n(t)$, the Hilbert transform is calculated to obtain its unilateral spectrum, and suppose the center frequency of each $u_n(t)$ is ω_n , the spectrum of each $u_n(t)$ is modulated to the respective estimated center frequency [30]. The calculation process is as follows:

$$\left[\left(\delta(t) + \frac{j}{\pi t} \right) * u_n(t) \right] e^{-j\omega_n t} \quad (3)$$

where $*$ is the convolution operation. To obtain the optimal solution of constrained variational problems in (1), the Lagrange multiplier and penalty term are introduced. Specifically, the following expression is obtained as:

$$\begin{aligned} L(\{u_n\}, \{\omega_n\}, \lambda) = & \\ \alpha \sum_N \left\| \partial_t \left[\left(\delta(t) + \frac{j}{\pi t} \right) * u_n(t) \right] e^{-j\omega_n t} \right\|_2^2 + & \\ \left\| f(t) - \sum_N u_n(t) \right\|_2^2 + \left\langle \lambda(t), f(t) - \sum_N u_n(t) \right\rangle & \end{aligned} \quad (4)$$

where α is penalty term, λ is Lagrange multiplier.

Combined with alternate direction method of multipliers (ADMM), the Parseval/Plancherel Fourier isometry under the L2-norm is used to convert the u_n and ω to frequency domain [30]. The iterative formulas of $\hat{u}_n(\omega)$ and ω_n , are expressed as follows:

$$\begin{aligned} \hat{u}_n^{m+1}(\omega) & \\ \leftarrow \frac{\hat{f}(\omega) - \sum_{i < n} \hat{u}_i^{m+1}(\omega) - \sum_{i > n} \hat{u}_i^m(\omega) + \frac{\hat{\lambda}^m(\omega)}{2}}{1 + 2\alpha(\omega - \omega_n^m)^2} & \end{aligned} \quad (5)$$

and the ω_n^{m+1} is updated as

$$\omega_n^{m+1} \leftarrow \frac{\int_0^\infty \omega |\hat{u}_n^{m+1}(\omega)|^2 d\omega}{\int_0^\infty |\hat{u}_n^{m+1}(\omega)|^2 d\omega} \quad (6)$$

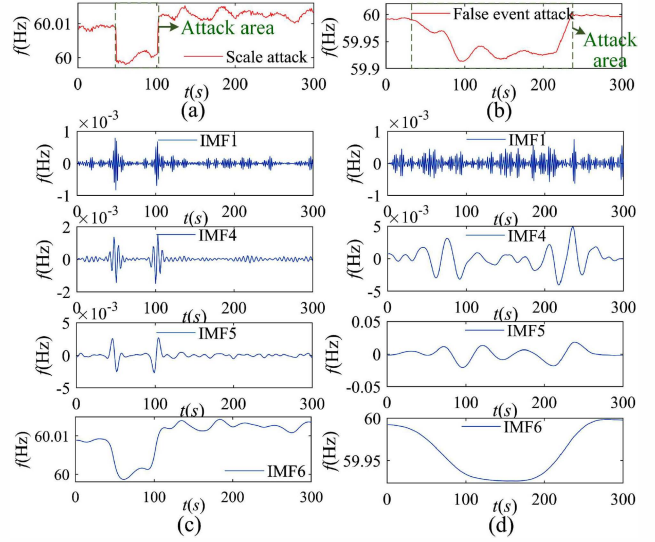


Fig. 1. Example of the signal decomposed by VMD. (a) The scaling attack, (b) The frequency shock attack, (c) The VMD result of (a), (d) The VMD result of (b).

where the $\hat{u}_n(\omega)$ is Fourier transform of $u_n(t)$, ω is the center frequency of $\hat{u}_n(\omega)$, $\hat{f}(\omega)$ is Fourier transform of $f(t)$, $\hat{\lambda}(\omega)$ is Fourier transform of $\lambda(t)$. To simplify the calculation, the gradient descent method is used to solve $\hat{\lambda}(\omega)$, which can be expressed as

$$\hat{\lambda}^{m+1}(\omega) \leftarrow \hat{\lambda}^m(\omega) + \beta \left(\hat{f}(\omega) - \sum_N \hat{u}_n^{m+1}(\omega) \right) \quad (7)$$

where β is the quadratic penalty term, which can improve the convergence. Thereafter, the $u_n(t)$ is obtained by the inverse Fourier transform of $\hat{u}_n(\omega)$.

Here, the number of decompositions N should not be too small to avoid incomplete decomposition or too large to avoid false components. In this article, the N is optimally set to 6 from the interval [3, 8], which means 6 IMF_i components are decomposed, where $i = 1, 2, \dots, 6$.

To show the decomposition effect of VMD, an example of two different cyber-attack frequency signals is presented in Fig. 1, including scaling and false event attacks. In scaling attack, the magnitude of a certain time interval is changed and deviated [12]. And the purpose of the false event attack is to cause a false response by injecting a false frequency event into the measurement data. Compared with Fig. 1(a) and (c), it can be seen that the start and end time components of scaling attack are detected in IMF_5 of Fig. 1(c). Meanwhile, the changing trend of false event attack is reflected in the residual component IMF_6 . For the false event attack, the oscillation model is extracted as can be seen from IMF_1 and IMF_5 between 50 to 150 s in Fig. 1(d). Therefore, the deterministic features are expected to be extracted from the $u_n(t)$.

B. Feature Extraction

After obtaining the IMFs of different attacked synchrophasor data, the distinctive attack features are extracted for attacked

synchrophasor data identification. Specifically, four types of features are used including two statistical features, and another two from the time and frequency domain, respectively.

The first feature (F_1) is the kurtosis index, which is sensitive to transient signals, thus it can reflect the degree of nonstationarity of each IMF. For IMF $_i$ of length n , the kurtosis is defined as

$$Ku_i = \frac{\frac{1}{n} \sum_{j=1}^n (m_j - \bar{m})^4}{\left(\frac{1}{n} \sum_{j=1}^n (m_j - \bar{m})^2\right)^2} \quad (8)$$

where m_j is the j th value of IMF $_i$, and \bar{m} is the average value of IMF $_i$.

If Ku_i is positive, it means that IMF $_i$ has obvious peak characteristics, which is called super-Gaussian distribution. If Ku_i is negative, it means that IMF $_i$ has no obvious impact or pulse signal, which is called sub-Gaussian distribution.

The second feature (F_2) is envelope entropy, in which the distribution of sources-information can be analyzed. The information entropy of each IMF envelope is a measure of the overall distribution of the signal. For each IMF $_i$, the envelope entropy can be calculated as

$$\begin{cases} Ee_i = -\sum_{j=1}^n (p_j \cdot \ln p_j) \\ p_j = E_{ij}(t) / \sum_{j=1}^n E_{ij}(t) \\ \sum_{j=1}^n p_j = 1 \end{cases} \quad (9)$$

where $E_{ij}(t)$ is the envelope signal of IMF $_i$ obtained by Hilbert transform, Ee_i is the envelope entropy of IMF $_i$. Generally, more uniform the distribution of variables in IMFs, smaller envelope entropy value of Ee_i .

The statistical characteristics of attack signals can be extracted by using Ku_i and Ee_i . Then, the time and unique frequency fingerprints are extracted to increase the diversity of features.

The third feature (F_3) is the FFT of $f(t)$. The frequency domain features after removing the main trend term can be used as fingerprints for synchrophasor data. Combined with the result of VMD, IMF $_6$ is the residual component that represents the main trend of the attacked signal. Therefore, frequency spectrum fingerprint can be obtained by applying the Fast Fourier Transform (FFT) to the detrending synchrophasor data, which can be calculated as

$$f_1(\omega) = \sum_{\tau=0}^{N_n-1} (f(\tau) - \text{IMF}_6(\tau)) e^{-j \frac{2\pi}{N_n} \tau k} \quad (k = 0, 1, \dots, N_n - 1) \quad (10)$$

where the N_n is the length of signal $f(\tau) - \text{IMF}_6(\tau)$, $\tau \in t$.

The fourth feature (F_4) is the original signal $f(t)$. All the features can be expressed as follows: $\{S^m\} = \{Ku_i, Ee_i, f_1(\omega), f(t)\}$, where $m = 1, 2, 3, 4$ denotes the order of four features.

To show the difference of designed features, two visual examples of the extracted features from the attacked signal are shown in Figs. 2 and 3. The scaling and replace attacks are used in Figs. 2 and 3, respectively [12], [32].

For the replace attack, the motivation is to mix the source ID, where a certain time interval is replaced by the data from the same WAMS within the same time range [32]. In Figs. 2(b)

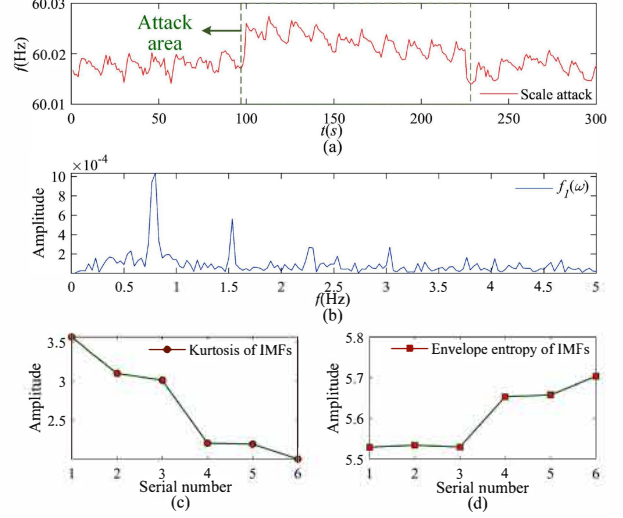


Fig. 2. Visual example of four features for scaling attack, (a) Scaling attack signal, (b) FFT of the original signal removing IMF $_6$, (c) Kurtosis of IMFs, (d) Envelope entropy of IMFs.

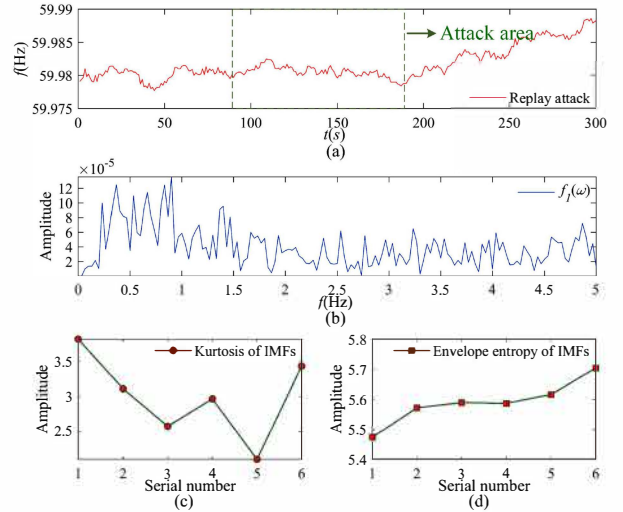


Fig. 3. Visual example of four features for a replacement attack, (a) Replace attack signal, (b) FFT of the original signal removing IMF $_6$, (c) Kurtosis of IMFs, (d) Envelope entropy of IMFs.

and 3(b), the $f_1(\omega)$ is the spectrum of the attack signal after removing IMF $_6$, which highlights the features of the attack signal. Theoretically, the functions of kurtosis and envelope entropy are complementary. In (c), (d) of Figs. 2 and 3, it also can be found that their changing trends are opposite to each other. Obviously, compared with Figs. 2 and 3, it can be found that the shape and value of these four features are different, thus providing a richer feature space from multiple aspects.

III. CYBER-ATTACK IDENTIFICATION VIA MULTIFUSION SVM

A. Principle of SVM

To achieve accurate classification of different attack signals, an efficient classifier is required. The SVM has strong learning ability and generalization ability, it is suitable for solving high

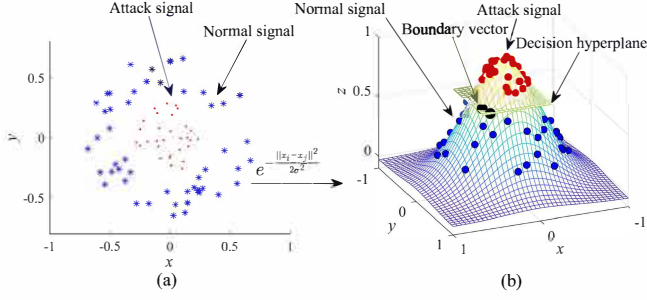


Fig. 4. Principle of kernel SVM classifier. (a) low-dimensional space, (b) high-dimensional space.

dimensional and nonlinear classification problems [33], [34]. Therefore, the SVM is selected to classify four features.

In SVM, given a set of feature samples $D = \{S^m, y_i\}$, where $i = 1, 2, \dots, n$, y_i is the label of feature S^m . If S^m is linearly separable, the objective of SVM is to find a hyperplane to maximize the distance between different classes. The definition of classification hyperplane can be obtained as

$$w^T S^m + b = 0 \quad (w \in R^n, b \in R). \quad (11)$$

However, if S^m is linearly inseparable, a kernel function is needed to map the sample to a high-dimensional feature space. This high-dimensional space is expected to be linearly separable. The most commonly used kernel function is the radial basis function (RBF), which can be defined as

$$K_{\text{RBF}}(s_i^m, s_j^m, \sigma) = \exp\left\{-\frac{\|s_i^m - s_j^m\|^2}{2\sigma^2}\right\} \quad (12)$$

where σ represents the kernel parameter of RBF, s_i^m and s_j^m are samples from S^m , respectively.

The principle of the kernel SVM classifier is shown in Fig. 4. It can be intuitively seen this classification process, where the kernel function maps the linearly inseparable samples from a low-dimensional space into a high-dimensional space to make the samples linearly separable. Particularly, the boundary vector determines the classification performance of SVM. Therefore, it is worth mentioning that the performance of kernel function and the choice of kernel function will directly affect the locations of boundary vectors.

B. Proposed Multifusion SVM

As mentioned above, the kernel function is crucial to the performance of SVM. It is found that the local and global characteristics of different kernel functions are different [35]. To improve the performance of SVM, different kernel functions can be combined according to Mercer's theorem [36]. Based on this consideration, the linear combined multikernel (LCM) method is first proposed to fuse multiple features, which can be expressed as

$$\begin{cases} K_{\text{LM}}(s_i^m, s_j^m) = \sum_{m=1}^4 \gamma_m K_{\text{RBF}}(s_i^m, s_j^m, \sigma_i) \\ \text{s.t. } \sum_{m=1}^4 \gamma_m = 1 \end{cases} \quad (13)$$

where K_{RBF} denotes RBF kernel, s_i^m represents the i th element of m th feature in S^m , σ_i represents the kernel parameter, γ_m denotes the weights of K_{RBF} . As can be seen, different features are mapped using different kernel functions in the proposed LCM-SVM.

For different features, the proposed LCM method uses different kernel functions and parameters. Meanwhile, the importance of different features is achieved by weights γ_m . This means that each feature can match the most suitable kernel functions, thus a distinguishable hyperplane can be constructed.

It is found that the classification effect of different kernel functions is often complementary for a certain feature. For example, the RBF kernel has better local characteristics while the polynomial kernel (PK) has better global characteristics. Additionally, the factors that affect the SVM classification are the eigenvectors between hyperplane boundaries.

Based on the above discussion, a new multifusion SVM is further proposed according to LCM-SVM. In MSVM, two kernel functions with different parameters and weights are used for each feature. One of the kernel functions is used for mapping and the other is expected to adjust the boundary vector. In this way, the combination of kernel functions for each feature is optimal. Based on the LCM, the novel combined multikernel functions are redefined as

$$\begin{cases} K_{\text{MF}}(s_i^m, s_j^m) = \sum_{m=1}^4 \{\mu_m K_1^m(s_i^m, s_j^m, p_{m,1}) + \varepsilon_m K_2^m(s_i^m, s_j^m, p_{m,2})\} \\ \text{s.t. } \sum_{m=1}^4 (\mu_m + \varepsilon_m) = 1 \text{ and } \mu_m > \varepsilon_m \end{cases} \quad (14)$$

where K_1^m and K_2^m are two different LCM functions used for the m th feature, $p_{m,1}$ and $p_{m,2}$ are the kernel parameters of K_1^m and K_2^m , respectively, μ_m and ε_m are their weights.

In (14), K_1^m is considered as the primary Kernel. The second kernel K_2^m is called calibration kernel function, which is used to repair the boundary vector. A smaller weight ε_m is assigned to K_2^m to limit its impact on K_1^m .

To learn the optimal classification hyperplane, the optimization framework of MSVM is introduced as follows:

$$\begin{aligned} \min_{\omega, b, \xi_i} & \left\{ \frac{\|\omega\|^2}{2} + C \sum_{i=1}^n \xi_i^2 \right\} \quad (\xi_i \geq 0, i = 1, \dots, n) \\ \text{s.t. } & y_i (w^T K_{\text{MF}}(s_i^m, s_j^m) + b) \geq 1 - \xi_i \end{aligned} \quad (15)$$

where ω denotes the weight vector, and b denotes the bias term of the decision plane, respectively, ξ_i is the slack variable, $C \geq 0$ is the penalty coefficient.

The optimal classification hyperplane can be obtained via partial derivatives from dual Lagrange function. After obtaining the parameters, for the new synchrophasor data z , the obtained decision function in the high-dimensional feature space is

$$\hat{y} = \text{sign}(w^T K_{\text{MF}}(s_i^m, z) + b). \quad (16)$$

Then, the label of each input signal can be determined by MSVM.

TABLE II
PERFORMANCE UNDER DIFFERENT KERNEL FUNCTIONS

Kernel	Optimal kernel combination ($S_1 + S_2 + S_3 + S_4$)	Accuracy (%)
K_1^m	0.1PK+0.35SK+0.4RBF+0.15SK	58.46
	0.3 SK +0.2PK+ 0.4 PK +0.1SK	84.17
	0.25RBF+ 0.25RBF+ 0.25RBF+0.25SK	86.36
	0.25RBF+ 0.25RBF+ 0.25RBF+ 0.25RBF	90.95
K_2^m	0.035RBF+0.015SK+0.025PK+ 0.025RBF	92.06
	0.02SK+0.03PK+0.025RBF+ 0.025RBF	92.79
	0.03RBF+ 0.04RBF+ 0.02RBF+ 0.01RBF	93.56
	0.01SK+0.03PK+0.02SK+0.04PK	93.87

TABLE III
OPTIMAL KERNEL COMBINATION FOR FEATURES

Features	Optimal kernel combination $K_1^m + K_2^m$
S_1	RBF+ SK
S_2	RBF + PK
S_3	RBF + SK
S_4	RBF + PK

C. Parameter Selection for MSVM

MSVM is a parameter sensitive method, which means that its parameter selection is critical for attack detection. According to its structure, the process of parameter optimization can be divided into two steps, including kernel selection optimization and parameter optimization.

Step 1: Finding the optimal combination of K_1^m and K_2^m

To verify the effect of multiple combinations of kernel functions, different kernel functions K are tested in K_1^m and K_2^m , respectively. To simplify the calculations, three commonly used kernel functions are used in this test, including RBF, PK, and Sigmoid Kernel (SK) functions. Results under these three kernels and the corresponding kernel parameters are listed in Table II.

Here, we first select kernels for K_1^m . After a satisfactory accuracy is obtained, then the K_2^m is further debugged based on the selected K_1^m . It should be notable that the weight coefficient can be further optimized in step 2.

As listed in Table II, the kernel functions have a greater impact on the performance of MSVM. Particularly, the MSVM obtains 90.95% accuracy when all the kernels are set to RBF in K_1^m . Meanwhile, the accuracy has improved by nearly 3% when K_2^m is used, indicating that the SK and PK help to the performance improvement of the MSVM. After some trial and error, the final selected kernel functions are listed in Table III.

Step 2: Finding the weight combination of different kernel functions and parameters

In the proposed method, eight weights are assigned to different kernel functions. To avoid getting stuck in the local minimum, the particle swarm optimization (PSO) algorithm is utilized to find the optimal kernel weights and kernel parameters. Specifically, the parameters to be optimized are set to the position of the particle. The classification error of the VMD-MSVM is

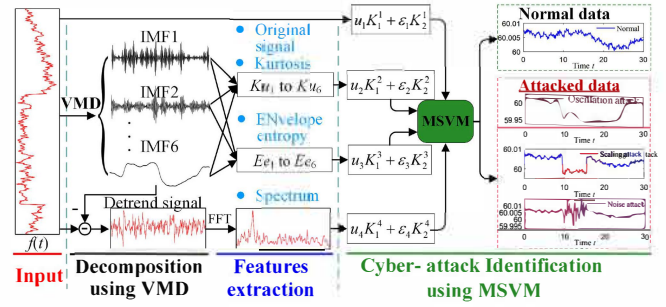


Fig. 5. Overall structure of the proposed VMD-MSVM.

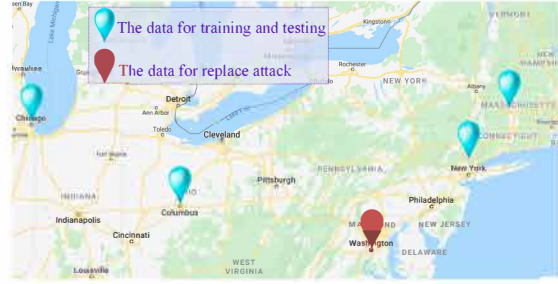


Fig. 6. Locations of synchrophasor data.

recorded as a fitness function in PSO. Then, the parameters can be optimized automatically.

D. Proposed VMD-MSVM Framework

The overall structure of the framework is shown in Fig. 5. It shows that the cyber-attack identification of synchrophasor data can be divided into three following steps:

- 1) *Cyber-Attack Based Synchrophasor Data Decomposition:* The IMFs are extracted from the input $f(t)$ using VMD.
- 2) *Feature Extraction:* Four features $F_1 - F_4$ are extracted as $\{S^m\} = \{Ku_i, Ee_i, f_1(\omega), f(t)\}$. The two statistics domain features are designed from the IMFs, including the Kurtosis and Envelope entropy of IMFs. The other two features are developed from the time and frequency domains.
- 3) *Identification Using MSVM:* Combining all these four features, the features of different domains are fused and mapped using the proposed MSVM. The type of cyber-attack synchrophasor data is then identified.

Since single kernel SVM is vulnerable to noise and outliers, the multidimensional features can improve the classification accuracy. Therefore, the proposed VMD-MSVM framework is suitable for multidimensional features classification. Next, the performance of the proposed VMD-MSVM will be further verified.

IV. EXPERIMENT

To verify the actual detection effect of the proposed VMD-MSVM, the synchrophasor frequency data in FNET/Grیده sever collected from five locations in eastern interconnection

TABLE IV
PERFORMANCE OF SINGLE FEATURE AND MULTIFEATURE FUSION

Input feature for the model	Accuracy (%)	Test time per sample (ms)
F_1 : Kurtosis Index	75.23	16.426
F_2 : Envelope Entropy	75.53	16.424
F_3 : FFT of $f(t)$	85.73	16.435
F_4 : Original Signal	71.62	0.036
Multi-feature Fusion	95.64	16.659

(EI) are used as an example, as shown in Fig. 6. Here, six different types of cyber-attacks are selected according to [17], [37], including noise, scaling, data loss, replace, false event (such as generation trip), and oscillation attack. For the replace attack, the data from one location is reserved as a replacement attack signal as shown in Fig. 6. The difference between the false event and oscillation attacks is that the false event and the low-frequency oscillation component are injected into synchrophasor data.

Using the actual frequency data, 3000 samples are generated for each type of attack by simulation. Under a 10 Hz reporting rate, each sample is truncated with a 30 s window length, which corresponds to a length of 300. Additionally, the samples are divided into three categories including training, verification, and testing dataset during the model validation. Utilizing the PSO method, the optimized parameters are selected as follows: $u_m = [0.174, 0.181, 0.129, 0.275]$, $\varepsilon_m = [0.035, 0.072, 0.082, 0.052]$. The penalty coefficient C is set to 2000. The kernel parameters of K_1^m and K_2^m are set to: $K_1^m = \{\text{RBF}(6.1), \text{RBF}(0.86), \text{RBF}(7.92), \text{RBF}(0.82)\}$, and $K_2^m = \{\text{SK}(1.51, 1.51), \text{PK}(1, 1.06), \text{SK}(2.34, 2.34), \text{PK}(1, 1.18)\}$, respectively.

A. Performance of Multifeature Fusion in MSVM

In MVSM, four features are fused by different kernels. To verify the effectiveness of multifeature fusion, each feature is fed into the SVM and tested separately. In this case, it should be noted that, the number of parameters is reduced, and the grid search method can be used to optimize parameters. The test is under 5 mHz attack strength and 500 training samples are used, where the result is listed in Table IV.

As can be seen from Table IV, the model with F_3 obtained 85.73% performance, and the performance with the original signal is the lowest. The time cost of the first three features ($F_1 - F_3$) is similar. The reason is that the VMD is required to be calculated first, then the statistical features can be implemented. Combined with all the features, multifeature fusion achieved 95.64% accuracy with a minimally time cost raise. The results indicate the effectiveness of the MSVM.

B. Performance Comparison With Different SVMs

To compare the effects of the proposed MSVM framework, the original SVM and LCM-SVM are tested separately. Additionally, different cyber-attack strengths are used to test the sensitivity. Considering that the error of frequency measurement equipment is generally lower than 5 mHz, thus the minimum attack strength is set to 5 mHz. The strength under 10 and

TABLE V
CLASSIFICATION ACCURACY BY DIFFERENT FRAMEWORKS

SVM methods	Accuracy(%)			Test time per sample (ms)
	5 mHz	10 mHz	20 mHz	
Original DVM	90.71	94.08	93.97	0.038
LCM-SVM	94.90	95.67	96.22	0.039
MSVM	95.64	96.96	96.51	0.067

20 mHz are also tested. In this test, 500 samples are randomly selected as training data. To make a fair comparison, all the SVM methods are optimized by using PSO. The optimized kernel parameters of LCM-SVM are: $\gamma_m = \{0.36, 0.31, 0.19, 0.14\}$; $K_{LM} = \{\text{RBF}(6.58), \text{RBF}(0.72), \text{RBF}(7.85), \text{RBF}(1.72)\}$. The accuracy comparison results for different frameworks are listed in Table V. All the input features are the same for different SVMs.

It can be seen from Table V that the original SVM has the lowest accuracy at different attack strengths. The LCM-SVM has 94.90% accuracy, which is nearly 4.2% higher than the original SVM under 5 mHz attack strength. Moreover, the MSVM has the highest classification accuracy among different SVM frameworks, indicating the effectiveness of the calibration kernel K_2^m . The test time of MSVM is higher due to multikernel computing. However, real-time can still be satisfied because the test time is less than 0.1 ms.

C. Comparison With DT, kNN, and ANN

To compare the performance of MSVM with some common classification algorithms. Three different classification frameworks are selected, including the VMD-DT [14], VMD-ANN, and VMD k-Nearest Neighbors (VMD-kNN) [38]. To match feature dimensions, the input features S^m are stitched together for VMD-ANN, VMD-DT, and VMD-kNN. In this case, 500 training samples are used.

DT classifies samples by Gini index minimization and the depth of DT is a key parameter. A DT model based on scikit-learn is used and the depth of 1–20 is tested. As shown in Fig. 7(a), when the depth is greater than 12, the verification error rate tends to be stable, therefore, the depth of DT is optimally selected as 12.

ANN establishes the mapping of input and output through multilayer perceptron. In ANN, the number of nodes in each layer and the number of layers are the main parameters for the improvement of detection results. In this experiment, a three-layer ANN based on MATLAB's toolboxes is used, its hidden nodes are optimally by grid search method and set to 300 finally, and using mean squared normalized error performance function. The mean squared error of ANN is shown in Fig. 7(b), when 218 epochs are iterated, the performance of ANN is best.

In kNN, the key parameter is the number of neighbors of the test sample. Euclidean distance is used to measure the distance between samples, then find K samples closest to test sample in the training data set, select the largest number of labels in K neighbors as the label of the test sample. It is a supervised method, the number of neighbors needs to be set manually.

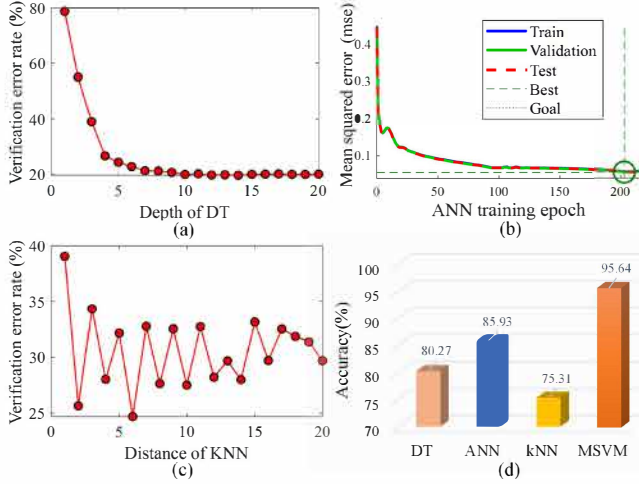


Fig. 7. Comparison results with different identification frameworks. (a) Error rate of DT at different depths. (b) Error rate of ANN with different training epoch. (c) Error rate of KNN with different distance. (d) Accuracy of different classifiers.

TABLE VI
TIME COST EACH SAMPLE FOR A DIFFERENT FRAMEWORK

Identification framework	Test time per sample (ms)
VMD-DT	16.609
VMD-ANN	16.611
VMD-kNN	16.606
VMD-MSVM	16.659

Different number of neighbors of kNN is tested and the result is shown in Fig. 7(c), and optimally selected as 6.

The accuracy is shown in Fig. 7(d), the time cost of different identification frameworks is also listed in Table VI. As can be seen from Fig. 7(d), the VMD-ANN reaches 85.93%, which performs better than VMD-DT and VMD-kNN. The kNN consumes less time for calculation because it has low time complexity. However, the accuracy of kNN is still 10.62% lower than the VMD-DT. The result shows that the kNN and DT are difficult to deal with the identification of complex attack signals. Meanwhile, it can be seen that the proposed VMD-MSVM has better performance even under six types of cyber-attack scenarios. This reason is that MSVM can integrate multiple input information better using the proposed LCM functions.

D. Comparison With Some Advanced Methods

In recent studies about cyber-attack identification, some advanced hybrid methods have also been proposed. To compare with the performance with these advanced methods, three typical hybrid methods are selected, including discrete wavelet transform (DWT)-BP [23], EEMD-FFT-BP [27], Mathematical Morphology (MM)-gcForest [32]. The details about these methods are introduced as follows.

- 1) *DWT-BP*: DWT-BP framework used daubechies wavelet-based extraction method to decompose the synchrophasor frequency data into 6 components. Then trained a 2-layer BP neural network to identify the cyber-attack

TABLE VII
TIME COST EACH SAMPLE FOR A DIFFERENT FRAMEWORK

Framework	Accuracy (%)	Test time per sample (ms)
MM-gcForest	76.87	25.182
EEMD-FFT-BP	82.32	236.095
DWT-BP	85.87	1.154
EMD-MSVM	79.98	11.867
DWT-MSVM	87.81	1.218
VMD-MSVM	95.64	16.659

data. Among them, the hidden layer has 60 neurons and the ‘tansig’ function is used. The final layer has 7 neurons and the softmax function is used.

- 2) *EEMD-FFT-BP*: This framework used EEMD to decompose the synchrophasor frequency data into 9 IMFs. Then, the FFT is utilized to analyze the frequency spectrum of IMFs. And the FFT result is treated as the features for each data source. Afterward, a 2-layer BP neural network is trained, the number of neurons in the hidden layer was 80.

- 3) *MM-gcForest*: It used a high pass filter to eliminate trend (DC component) interference, then the synchrophasor frequency data is decomposed to obtain the intrinsic components through a MM method. Each synchrophasor frequency data is decomposed into 30 scales. After that, the sparsity trends and roughness values of the intrinsic components are calculated to establish the time–frequency sparsity mapping. Finally, the gcForest classifier is used to identify the cyber-attack.

In addition, considering that EMD and DWT are common methods for signal decomposition and feature extraction that suitable for the no-linear signal, the EMD-MSVM and DWT-MSVM are also selected to verify the detection performance. For fairness, the number of decomposition components is consistent. The detection results are listed in Table VII.

As can be seen from Table VII, the MM-gcForest obtains 76.87% accuracy, which is the lowest accuracy. This is because the accuracy of MM-gcForest decreases with the increasing of the classification categories-number and the amount of data. The accuracy of EEMD-FFT-BP is relatively 5.45% higher than MM-gcForest, but it consumes more time. The antinoise performance of EMD is limited because it is susceptible to modal mixing and endpoint effects. Benefitting from the multifeature fusion of MSVM, DWT-MSVM performs better than DWT-BP and obtains 87.81% accuracy. Besides, both the performance of DWT-BP and DWT-MSVM are lower than 88%. The reason is that the wavelet filter is not an ideal filter, this will lose some information during the feature extraction. VMD-MSVM achieves 95.64% accuracy because VMD can adaptively adjust the bandwidth of IMFs.

Overall, the proposed VMD-MSVM has achieved a good balance between the highest accuracy and running speed. Particularly, it has the highest accuracy compared with the other advanced methods, indicating that it is suitable for the detection of attack signals.

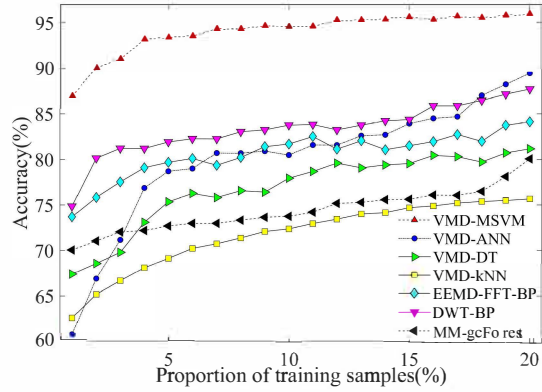


Fig. 8. Comparison of generalization ability under a different number of training samples.

E. Comparison of the Generalization Ability

The generalization and robustness ability of the model, namely the learning ability under different training samples, reflects the recognition results for unknown attack signals. To verify the generalization ability of the proposed method, we randomly select 1% to 20% of the sampling data from each attack category as the training data. The remaining samples are used for testing. If the model can get higher recognition accuracy with fewer training samples, it means that the practicability of the model is better because more information can be learned.

The accuracy under different ratios samples is recorded, as shown in Fig. 8. It shows that the VMD-kNN and MM-gcForest have lower robustness because the accuracy is less than 80% even with 20% training data. The accuracy of DWT-BP and VMD-ANN is 5% lower than VMD-MSVM. Conversely, the results reveal that the proposed VMD-MSVM has better generalization and robustness ability because it obtains the highest accuracy especially when the training data is greater than 4%.

V. CONCLUSION

To detect cyber-attacks on power systems, a multidomain feature fusion based VMD and multifusion SVM are proposed. Utilizing the decomposition modal functions, four distinctive features are extracted. The recognition results under different features indicate that the modal component IMFs contains unique attack components. Thereafter, four features from statistics, time, and frequency domains are fused and automatically learned based on the proposed MSVM. Using the actual synchrophasor data, the results of different single and multiple kernel functions show that combined kernel functions have a better learning ability. Moreover, these multiple kernels further optimize classification capabilities. Experiments with different attack strengths and training samples are conducted to verify the detection ability and robustness of the proposed VMD-MSVM. Compared with commonly used classifiers, the result shows that the VMD-MSVM has strong adaptability. The future work will focus on the optimization of model feature extraction to further reduce the time cost of the model.

REFERENCES

- [1] D. Wang, X. Wang, Y. Zhang, and L. Jin, "Detection of power grid disturbances and cyber-attacks based on machine learning," *J. Inf. Secur. Appl.*, vol. 46, pp. 42–52, 2019.
- [2] R. Jumar, H. Maaß, B. Schäfer, L. R. Gorjão, and V. Hagenmeyer, "Database of power grid frequency measurements," Jun. 2021, *arXiv:2006.01771v3*.
- [3] S. Saha, T. Roy, M. Mahmud, M. Haque, and S. Islam, "Sensor fault and cyber attack resilient operation of DC microgrids," *Int. J. Elect. Power Energy Syst.*, vol. 99, pp. 540–554, 2018.
- [4] C. Pei, Y. Xiao, W. Liang, and X. Han, "PMU placement protection against coordinated false data injection attacks in smart grid," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4381–4393, Jul./Aug. 2020.
- [5] R. Khan, K. McLaughlin, D. Lavery, and S. Sezer, "Analysis of IEEE C37.118 and IEC 61850-90-5 synchrophasor communication frameworks," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2016, pp. 1–5.
- [6] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, 2018.
- [7] 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 2019.
- [8] H.-M. Chung, W.-T. Li, C. Yuen, W.-H. Chung, and C.-K. Wen, "Local cyber-physical attack with leveraging detection in smart grid," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, 2017, pp. 461–466.
- [9] Y. Chakhchoukh and H. Ishii, "Enhancing robustness to cyber-attacks in power systems through multiple least trimmed squares state estimations," *IEEE Trans. Power Syst.*, vol. 31, no. 6, pp. 4395–4405, Nov. 2016.
- [10] Q. Wang, W. Tai, Y. Tang, and M. Ni, "Review of the false data injection attack against the cyber-physical power system," *IET Cyber-Phys. Syst.: Theory Appl.*, vol. 4, no. 2, pp. 101–107, 2019.
- [11] K. Sun, W. Qiu, W. Yao, S. You, H. Yin, and Y. Liu, "Frequency injection based HVDC attack-defense control via squeeze-excitation double CNN," *IEEE Trans. Power Syst.*, vol. 36, no. 6, pp. 5305–5316, Nov. 2021.
- [12] M. Yue, "Evaluation of a data analytic based anomaly detection method for load forecasting data," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2018, pp. 1–5.
- [13] M. N. Kurt, O. Ogundijo, C. Li, and X. Wang, "Online cyber-attack detection in smart grid: A reinforcement learning approach," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5174–5185, Sep. 2019.
- [14] K. Khanna, B. K. Panigrahi, and A. Joshi, "AI-based approach to identify compromised meters in data integrity attacks on smart grid," *IET Gener. Transmiss. Distrib.*, vol. 12, no. 5, pp. 1052–1066, 2018.
- [15] A. Jindal, A. Dua, K. Kaur, M. Singh, N. Kumar, and S. Mishra, "Decision tree and SVM-based data analytics for theft detection in smart grid," *IEEE Trans. Ind. Informat.*, vol. 12, no. 3, pp. 1005–1016, Jun. 2016.
- [16] M. Kalech, "Cyber-attack detection in SCADA systems using temporal pattern recognition techniques," *Comput. Secur.*, vol. 84, pp. 225–238, 2019.
- [17] 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.
- [18] J. Pei, J. Wang, and D. Shi, "Data-driven measurement tampering detection considering spatial-temporal correlations," in *Proc. IEEE 3rd Conf. Energy Internet Energy Syst. Integration*, 2019, pp. 2641–2646.
- [19] P. Priyanga S, K. Krithivasan, P. S, and S. Sriram V S, "Detection of cyberattacks in industrial control systems using enhanced principal component analysis and hypergraph-based convolution neural network (EPCA-HG-CNN)," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4394–4404, Jul./Aug. 2020.
- [20] H. Karimipour, A. Dehghantanha, R. M. Parizi, K.-K. R. Choo, and H. Leung, "A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids," *IEEE Access*, vol. 7, pp. 80778–80788, 2019.
- [21] H. Wang *et al.*, "Dynamic data injection attack detection of cyber physical power systems with uncertainties," *IEEE Trans. Ind. Informat.*, vol. 15, no. 10, pp. 5505–5518, Oct. 2019.
- [22] L. Wei, D. Gao, and C. Luo, "False data injection attacks detection with deep belief networks in smart grid," in *Proc. Chin. Automat. Congr.*, 2018, pp. 2621–2625.

- [23] 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.
- [24] D. Wilson, Y. Tang, J. Yan, and Z. Lu, "Deep learning-aided cyber-attack detection in power transmission systems," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2018, pp. 1–5.
- [25] M. R. Habibi *et al.*, "Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks," *IEEE Trans. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 5, pp. 5294–5310, Oct. 2021.
- [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.*, 2016, pp. 1–8.
- [27] S. Liu *et al.*, "Model-free data authentication for cyber security in power systems," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 4565–4568, Sep. 2020.
- [28] T. Aldwairi, D. Perera, and M. A. Novotny, "An evaluation of the performance of restricted Boltzmann machines as a model for anomaly network intrusion detection," *Comput. Netw.*, vol. 144, pp. 111–119, 2018.
- [29] W. Qiu *et al.*, "Cyber-attack identification of synchrophasor data via vmd and multi-fusion SVM," in *Proc. IEEE Ind. Appl. Soc. Annu. Meeting*, 2020, pp. 1–6.
- [30] K. Dragomiretskiy and D. Zosso, "Variational mode decomposition," *IEEE Trans. Signal Process.*, vol. 62, no. 3, pp. 531–544, Feb. 2013.
- [31] S. Shukla, S. Mishra, B. Singh, and S. Kumar, "Implementation of empirical mode decomposition based algorithm for shunt active filter," *IEEE Trans. Ind. Appl.*, vol. 53, no. 3, pp. 2392–2400, May/Jun. 2017.
- [32] Y. Cui, F. Bai, Y. Liu, P. L. 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.
- [33] R. T. Rockafellar, "A dual approach to solving nonlinear programming problems by unconstrained optimization," *Math. Program.*, vol. 5, no. 1, pp. 354–373, 1973.
- [34] J. Mercer, "Functions of positive and negative type and their connection with the theory of integral equations," *Philos. Transactions Roy. Soc.*, vol. 209, pp. 4–415, 1909.
- [35] G. F. Smits and E. M. Jordaan, "Improved SVM regression using mixtures of kernels," in *Proc. Int. Joint Conf. Neural Netw.*, vol. 3, 2002, pp. 2785–2790.
- [36] Q. Tang, W. Qiu, and Y. Zhou, "Classification of complex power quality disturbances using optimized S-transform and Kernel SVM," *IEEE Trans. Ind. Electron.*, vol. 67, no. 11, pp. 9715–9723, Nov. 2020.
- [37] H. M. Khalid and J. C.-H. 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.
- [38] E. M. de Lima Pinto, R. Lachowski, M. E. Pellenz, M. C. Penna, and R. D. Souza, "A machine learning approach for detecting spoofing attacks in wireless sensor networks," in *Proc. IEEE 32nd Int. Conf. Adv. Inf. Netw. Appl.*, 2018, pp. 752–758.