Cyber Spoofing Detection for Grid Distributed Synchrophasor Using Dynamic Dual-Kernel SVM

Wei Qiu, *Graduate Student Member, IEEE*, Qiu Tang, Kunzhi Zhu, Wenxuan Yao, *Senior Member, IEEE*, Jun Ma, and Yilu Liu, *Fellow, IEEE*

***Abstract*—Cyber spoofing with distributed synchrophasor adversely affects the decision-making and situational awareness of the power grid. To detect the spoofing trail, this letter proposes a composite signature-based cyber spoofing detection methodology. The intrinsic principal modes are first extracted from the distributed synchrophasor data. Then, multiple signatures of different intrinsic model components are derived to quantify the spoofing. Thereafter, the dynamic dual-kernel support vector machine is proposed to identify cyber spoofing using multiple signatures. Multiple experimental results using six spoofing methods have verified the validity of the methodology.**

***Index Terms*—Cyber spoofing, distributed synchrophasor, dynamic dual-kernel support vector machine.**

I. Introduction

DUE TO the rising demand for transmission and callback of grid measurements, the number of synchronized measurement devices that collect distributed synchrophasor data from different locations is increased, making it vulnerable to be tampered by the False Data Injected Attack (FDIA). FDIA is an attack method where data is manipulated and modified by adversaries. For example, the source authentication can be confused by high similarity false measurement value injected [1]. The cyber spoofing attack will cause equipment and economic losses to the power system. Between 2011 and 2014, it is reported that a total of 362 power interruption reports that are related to cyber attack in the USA [2].

Manuscript received March 23, 2020; revised June 23, 2020 and September 4, 2020; accepted October 2, 2020. Date of publication November 19, 2020; date of current version April 21, 2021. This work was supported in part by the Engineering Research Center Program of the National Science Foundation and DOE under NSF Award EEC-1041877; in part by the CURENT Industry Partnership Program; and in part by the Postgraduate Scientific Research Innovation Project of Hunan Province. Paper no. PESL-00085-2020. *(Corresponding authors: Qiu Tang; 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, Kunzhi Zhu, and Jun Ma are with the College of Electrical and Information Engineering, Hunan University, Changsha 410082, China (e-mail: tangqiu@hnu.edu.cn; zhukunzhi@hnu.edu.cn; 19090277@hnu.edu.cn).

Wenxuan Yao was with the Energy and Environmental Sciences Directorate, Oak Ridge National Laboratory, Oak Ridge, TN 37830 USA. He is now with the College of Electrical and Information Engineering, Hunan University, Changsha 410082, China (e-mail: ywxhnu@gmail.com).

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

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSG.2020.3039411.

Digital Object Identifier 10.1109/TSG.2020.3039411

Moreover, the purpose of cyber spoofing detection is to protect the reliability, consistency, and availability of the measurement data. Most of the applications that use synchrophasor data for power grid situational awareness, such as oscillation analysis and event location [3], can be protected. In [4], the data packet can be hacked as the IEEE C37.118 lacks a perfect security mechanism. If the channel security characteristics are incomplete, even dedicated channels may still be attacked.

With the increasing sophisticate of FDIA, the state estimation methods based on the power system model are used to identify FDIA [2]. However, it requires the information of the system parameter and its performance will be degraded when the model differs from actual operation. Then, the model-free methods using the measurement values are developed, such as gcForest and Support Vector Machine (SVM) [1]. However, they are prone to being deceived because only a small amount of input information is considered. SVM also has limited learning ability because only single kernel is used. The power system faces cyber security challenges in three aspects, including the device, communication, and control center [5]. Based on this consideration, to detect the availability of data and prevent misuse of attack data in time, the FDIA detection method is urgently required.

In this letter, a cyber spoofing detection methodology is introduced using composite signature-based features of grid distributed synchrophasor. Specifically, a Dynamic dual-Kernel Support Vector Machine (DKSVM) is proposed to solve the defect of single kernel in SVM. The advantage of DKSVM is that multi-source signatures and multiple kernels are used.

II. Cyber Spoofing Detection Framework

Different characteristics are exhibited in various FDIAs, which means that the signatures of these Spoofing Synchrophasor Data (SSD) are different from the normal data. Under this scenario, the proposed methodology for SSD detection is depicted in Fig. 1(a).

Denoting the distributed synchrophasor value as $c(t)$. It can be seen that this framework includes three stages:

1) Feature extraction: the Variational Mode Decomposition (VMD) is utilized to decompose the $c(t)$ into multiple Intrinsic Principal Modes (IPMs) $v(t)$.
2) Combining with data $c(t)$, three signatures including the kurtosis, envelope entropy, and spectrum are calculated from the IPMs $v(t)$ in time and frequency domains.

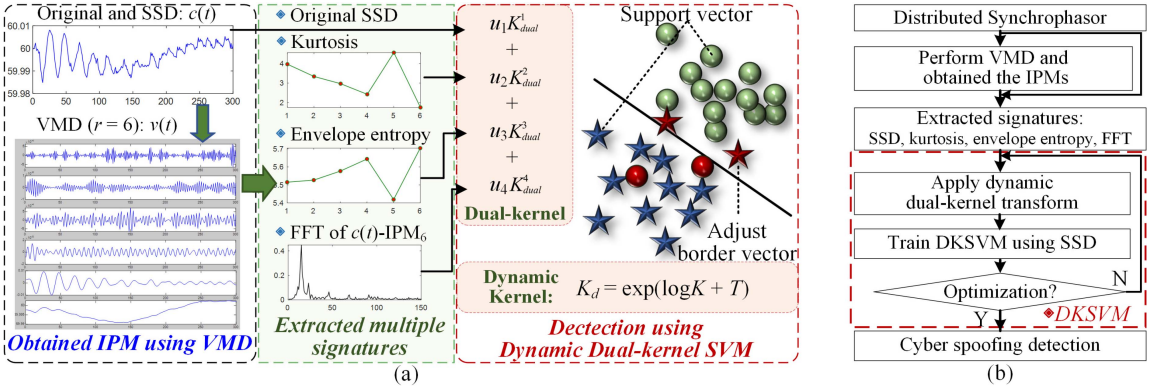

Fig. 1. The cyber spoofing detection framework. (a) Framework of VMD-DKSVM, (b) Flowchart of VMD-DKSVM.

3) SSD detection: Four signatures are transformed in the proposed dynamic dual-kernel space. The SSD can be identified from original data using the VMD-DKSVM methodology. As shown in Fig. 1(b), the parameters of DKSVM are then optimized and selected.

Here, to include as many different characteristics of spoofing as possible, six types of cyber spoofing methods are considered [6], [7], including the scaling (S1), noise (S2), data packet loss (S3), oscillation (S4), synchronous replacement (S5) and fake frequency disturbance (S6) spoofing.

III. Principle of the Cyber Spoofing Detection

A. Signature Extraction Using VMD

To extract the features from the SSD, a signal decomposition method is required. VMD is an adaptive method and suitable for the decomposition of non-steady state signals. Compared with the traditional Empirical Mode Decomposition (EMD), VMD overcomes the problems of end effect and modal aliasing. The primary objective of VMD is to decompose the synchrophasor signal $c(t)$ into multiple sub-signals $v(t)$. These sub-signals consist of spoofing components, which have the property of reproducing the input signal.

To obtain the IPMs, the following constrained variational problem should be satisfied, which can be written as

$$\min_{\{v_r\},\{\omega_r\}} \left\{ \sum_r \left\| \partial_t \left[v_+^r(t) \exp^{-j\omega_r t} \right] \right\|_2^2 \right\} \tag{1}$$

where the $v_+^r(t)$ is the analytic signal of $v_r(t)$, the $v_r(t)$ denotes the rth IPM, the ∂_t denotes the partial derivative of time, the spectrum factor $\exp^{-j\omega_r t}$ is used to adjust the frequency band centered of each $v_r(t)$. This constrained problem should satisfy $\sum_r v_r(t) = c(t)$.

By solving this constrained problem, the IPMs can be extracted. To verify the decomposition effect of the VMD, an oscillator synchrophasor frequency spoofing with max amplitude 10 mHz is demonstrated in Fig. 2. The r is set to 6 which means 6 IPMs are decomposed. Compared with Fig. 2(c) and (d), (g) and (h), the shape and amplitude are similar, which indicating that the common IPMs of original data and SSD are extracted. It can be seen from Fig. 2(e) and (f) that the oscillator component has been extracted with the same amplitude.

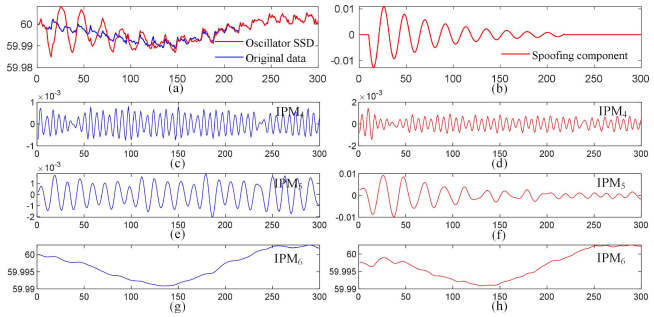

Fig. 2. The VMD result of oscillator spoofing. (a) The oscillator SSD and original data, (b) The oscillator spoofing component, (c) (e) and (g) are the 4th, 5th and 6th IPMs of oscillator SSD respectively, (d) (f) and (h) are the 4th, 5th and 6th IPMs of original data respectively.

After obtained the IPMs, different signatures are extracted. It is founded from [8] that patterns of the synchrophasor data will not change in the short term. To maximize the detection performance and ensure its robustness and adaptability, features from different domains are extracted to fully characterize the attack signal. Two statistical signatures are kurtosis, envelope entropy of each IPM which can be denoted as s_r, e_r respectively. Additionally, the frequency domain information of each signal has proved to be the unique fingerprints since the main trend term (called residual IPM component) of the signal is obtained [6]. Specifically, the spectrum signature f is calculated from the FFT of $c(t) - v_6(t)$, where the $v_6(t)$ is the residual IPM component.

It is emphasized that the spectrum and statistical signatures do not include time domain information. However, the shape change in the time domain can be used to distinguish several cyber spoofing methods, such as S1 and S3. Therefore, the original SSD is also selected as one of signatures. Finally, four signatures $s_n = \{s_r, e_r, f, c(t)\}, n = 1, 2, 3, 4$ are designed as the input of DKSVM. It should be notable that if more attacks need to be detected, more features can be designed and a larger number of training data is required to learn the model parameters.

B. Proposed DKSVM

To fully integrate and identify the extracted signatures, a dynamic dual-kernel SVM is proposed to detect the cyber spoofing. The advantage of the DKSVM is that multiple kernel

function can be utilized to map each input signature to get higher accuracy while only a single dedicated kernel is used in generally SVM. Concretely, given the input vectors as $I = \{s_n^i, y_i\}$, where the s_n^i is the ith samples and the y_i is the label of s_n^i. The dual-Kernel SVM (KSVM) is first proposed, which the dual-kernel is defined as

$$K(s_n^i, s_n^j) = \sum_{n=1}^{4} \mu_n K_{dual}^n(s_n^i, s_n^j) \tag{2}$$

$$\mu_n K_{dual}^n = (\mu_n - \lambda)K_{d1}^n + \lambda K_{d2}^n \tag{3}$$

where the μ_n is the coefficient of different kernels and it satisfies $\sum_{n=1}^{4} \mu_n = 1$. The K_{dual}^n is the dual-kernel and it consists of two different sub-kernels K_{d1} and K_{d2}. The $\lambda \subset [0, 0.1]$ is the coefficient of sub-kernels. The sub-kernel K_{d1}^n is used as the primary kernel, and K_{d2}^n is used to correct the misclassified support vectors in K_{d1}^n.

Moreover, it is notable that two signatures of I have a certain similarity if they belong to the same cyber spoofing class. Therefore, a label information of the training samples can be incorporated into the prediction of KSVM [9]. Here, the dynamic KSVM is further proposed to use the label information dynamically. The dynamic dual-kernel for training process can be expressed as

$$K_d(s_n^i, s_n^j) = \exp(logK(s_n^i, s_n^j) + T) \tag{4}$$

$$T(s_n^i, s_n^j) = \begin{cases} \beta, & y_i = y_j \\ 0, & y_i \neq y_j \end{cases} \tag{5}$$

where the $T(s_n^i, s_n^j)$ is the dynamic ideal kernel, β is the dynamic factor and it represents the weight information of the label. Using the Neumann divergence [9], the new synchrophasor samples of the DKSVM is calculated as

$$K_d(s_n^p, s_n^q) = -K(s_n^p, s_n^q) + K(s_n^p, s_n^q)SK(s_n^i, s_n^j) \tag{6}$$

where the $s_n^p, s_n^q \subset I$ are the prediction samples. The $S = K^{-1}(K_d(s_n^i, s_n^j) + K)K^{-1}$. Finally, the cyber spoofing detection decision function can be obtained as

$$\bar{y} = sign(\boldsymbol{W}^{\boldsymbol{T}} K_d(s_n^p, s_n^q) + b) \tag{7}$$

where the $\boldsymbol{W}^{\boldsymbol{T}}$ and b denote the learned weight vector and bias term respectively.

IV. Experiments and Analysis

To verify the proposed cyber spoofing detection methodology, the distributed synchrophasor data of four Frequency Disturbance Recorders (FDRs) in FNET/GridEye are collected at different operating points as shown in Fig. 3. More importantly, some disturbance events, such as generation trip and load shedding, have been included in the training data since the actual synchrophasor data is collected. Thus this method can identify different power system configurations. The data are collected at three time nodes including the first day of January (D1), March (D2), and May (D3) respectively. In each day, 3000 samples are collected and the duration of each sample is 30 s with 10 Hz reporting rate. Seven types of data are used to classify including one type of normal data and six types of spoofing synchrophasor data S1-S6. Based on the numerical model in [6], [7], the intensity (magnitude) and the duration time of the spoofing are randomly set. The length of each sample is 300. The duration time is set to $10\% - 90\%$ of the total length. The kernel parameters and coefficients of DKSVM are optimized by using particle swarm optimization. The number of IPMs is optimized set to 6 in VMD. Namely, 6 s_r, e_r of each SSD are calculated.

Fig. 3. Location of the distributed FDRs in FNET/GridEye.

TABLE I
Performance With Different Proportions of Training Data

Methods	Accuracy (%)				Hamming loss
	10%	30%	50%	70%	
$c(t)$-SVM	54.46	63.57	68.87	70.92	0.464
$c(t)$-DKSVM	55.13	63.94	69.05	71.17	0.463
VMD-SVM	89.25	92.79	94.41	94.39	0.107
VMD-KSVM	93.89	95.80	96.63	96.98	0.061
VMD-DKSVM	94.28	96.15	96.97	97.14	0.056

The kernels are selected as follows by some trials and fails: all the K_{d1}^n are set as Radial Basis Function (RBF) kernels, the K_{d2}^n are designated as Sigmoid, Polynomial and tanh kernels for $K_{d2}^1, K_{d2}^3, K_{d2}^4$ respectively, where the dual-kernel of e_r is not set. The corresponding λ is set to 0.01. The coefficients μ_n of dual-kernels are 0.15, 0.24, 0.15 and 0.46 respectively. The dynamic factor $\beta = 0.0015$.

A. Results With Different SVM Methodology

To verify the robustness of the proposed VMD-DKSVM, the SVM, KSVM, and DKSVM are compared under different proportions of training data, which means that the different number of training samples are used in the training process. The detection and hamming loss results are listed in Table I, which the input of $c(t)-$SVM and $c(t)-$DKSVM are $c(t)$. In Table I, $n\%$ training data means $n\%$ data from the 3000 samples are randomly selected. The hamming loss denotes the proportion of misidentification samples. A lower hamming loss means a better classifier. It can be inferred that the signatures derived from VMD can greatly improve the spoofing detection effect compared from the SVM and VMD-SVM, DKSVM and VMD-DKSVM. Moreover, the VMD-DKSVM obtained the 94.28% accuracy ever with only 10% training data. However, the VMD-SVM reaches 89.25%, which is 5% lower than VMD-DKSVM. As the training samples increase, the accuracy difference decreases due to the compression of the test sample space. Moreover, it is clear from Table I that the SVM method obtains the highest hamming loss while the VMD-DKSVM has the lowest value. This means that the proposed method has better attack recognition capability.

To verify the accuracy of different attacks, the confusion matrix is calculated as shown in Fig. 4. Both the number of observations and the accuracy are shown in each cell. The column on the far right are the precision and false discovery rate, respectively. The row at the bottom of the plot are

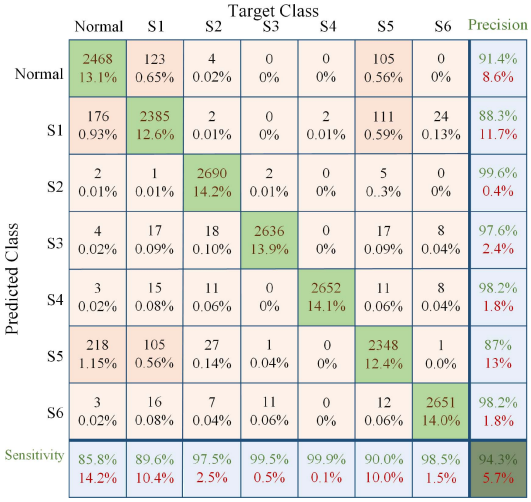

Fig. 4. The confusion matrix of the VMD-DKSVM when 10% data are used in training.

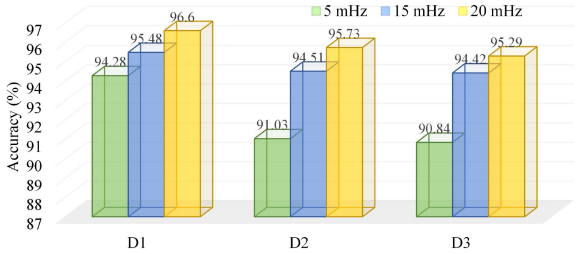

Fig. 5. The accuracy in different test time nodes with 10% training data.

TABLE II
PERFORMANCE COMPARISON OF MACHINE LEARNING METHODS

Methods	Accuracy (%)			Test time for each sampple (ms)
	5 mHz	10 mHz	20 mHz	
VMD-ANN	64.72	84.34	87.78	24.51
VMD-DT	78.20	82.67	86.65	24.52
MM-TF-GCF	50.49	56.48	64.07	27.18
VMD-DKSVM	94.28	95.48	96.60	24.66

the recall and false negative rate, respectively. It can be seen that the noise (S2), oscillation (S4), and fake frequency disturbance (S6) have higher precision. The performance of scaling (S1) and synchronous replacement (S5) are lower than the overall accuracy. In S1 and S5, more than 0.93% and 1.15% data are misidentified to normal data. The reason is because the shape of the S1 and S5 is very similar to the normal data when the attack intensity is small. The S4 has the lowest false negative rate with only 0.1% because the features can be efficiently extracted by VMD. However, the normal data obtains the 14.2% false negative rate. It indicates that the attack is prone to misidentification when the attack intensity is small. The overall accuracy reaches 94.3% shown in the bottom right means that the VMD-DKSVM has the potential to detect multiple attacks.

B. Results With Different Spoofing Intensity

The complexity of spoofing data is the key to verify the performance of VMD-DKSVM. Therefore, the accuracy under different spoofing intensity and time nodes are shown in Fig. 5. Meanwhile, three types of intensities including 5 mHz, 10 mHz, and 20 mHz are tested due to the measurement error of FDRs is generally lower than 5 mHz. It shows that as the spoofing intensity of SSD increases, the detection accuracy is further improved. From a time node perspective, the model detection accuracy changes stay within 1% even at D3 when the spoofing intensity higher than 5 mHz. This means that the VMD-DKSVM has profound robustness. To ensure long-term effectiveness, the VMD-DKSVM can train once every week using the latest measurement data.

C. Comparison With Other Machine Learning Methods

In the case, another three intelligent methods are used to identify the SSD, including the Artificial Neural Networks (ANN), Decision Trees (DT), MM-TF-GCF [1]. Table II summarized the accuracy and running time of different methods. When the spoofing intensity is 20 mHz, it shows that the accuracy of ANN and DT classifiers are higher than 86%, while the MM-TF-RFC is less than 70%. Additionally, the proposed VMD-DKSVM obtains the best performance under different intensities. The test time of VMD-DKSVM is 0.15 ms higher than ANN and DT due to the kernel calculation. However, the real-time performance can be satisfied because the time is far below 30 s.

V. CONCLUSION

In this letter, a composite signature-based methodology, which is composed of VMD and DKSVM, is proposed to detect the cyber spoofing in distributed synchrophasor. Utilizing the sync frequency data from FNET/GridEye, the experimental results under different intensity and time nodes reveal that the proposed methodology has high spoofing detection capability and robustness. This makes it suitable for data spoofing monitoring in distributed synchronized measurement devices.

REFERENCES

[1] Y. Cui *et al.*, "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.
[2] 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.
[3] J. Guo *et al.*, "Events associated power system oscillations observation based on distribution-level phasor measurements," in *Proc. IEEE PES T D Conf. Expo.*, 2014, pp. 1–5.
[4] 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)*, 2016, pp. 1–5.
[5] S. Aditya, K. Tanwir, and M. Amir, "Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies," *J. Mod. Power Syst. Clean Energy*, vol. 7, pp. 449–467, May 2019.
[6] 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.
[7] S. Pan, T. Morris, and U. Adhikari, "Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data," *IEEE Trans. Ind. Informat.*, vol. 11, no. 3, pp. 650–662, Jun. 2015.
[8] 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.
[9] B. Pan, J. Lai, and L. Shen, "Ideal regularization for learning kernels from labels," *Neural Netw.*, vol. 56, pp. 22–34, Aug. 2014.