


# Hybrid Data-Driven Based HVdc Ancillary Control for Multiple Frequency Data Attacks

Wei Qiu , *Student Member, IEEE*, Kaiqi Sun , *Member, IEEE*, Wenxuan Yao , *Senior Member, IEEE*, Weikang Wang , *Student Member, IEEE*, Qiu Tang , and Yilu Liu , *Fellow, IEEE*

**Abstract**—The high voltage direct current (HVdc) intertie has been applied to provide ancillary-services for ac grids, utilizing the real-time feedback from phasor measurement units (PMUs). However, PMU data communication is vulnerable to false data injection attacks (FDIA) due to protocol defects, thus the HVdc ancillary control and system stability will be threatened. To address this issue, this article proposes a novel HVdc control strategy based on a hybrid data-driven (HDD) methodology. The HDD methodology is first proposed to detect the types and duration time of multiple frequency attacks. Specifically, the Hilbert Huang transform (HHT) is used to decompose the frequency data, using variational mode decomposition instead of the traditional empirical mode decomposition, to extract data features. Second, a multikernel support vector machine is proposed to classify the attacked data based on the designed distinctive features from HHT. Meanwhile, the attacking duration time is decided using an unsupervised technique. Third, an HDD-based HVdc ancillary control strategy is established to eliminate the effect of FDIAs on the HVdc frequency response. Comprehensive experiments of HDD-based HVdc ancillary controls under different FDIAs suggest that the proposed HDD could fast and accurately classify the FDIAs, and the HDD-based HVdc ancillary control strategy could significantly suppress the impact of the FDIAs.

Manuscript received July 24, 2020; revised December 5, 2020 and February 1, 2021; accepted February 23, 2021. Date of publication March 3, 2021; date of current version August 20, 2021. This work was supported in part by the Engineering Research Center Program of the National Science Foundation, DOE under NSF Award No. EEC-1041877, in part by CURENT Industry Partnership Program, and in part by the Postgraduate Scientific Research Innovation Project of Hunan Province under Grant CX20200426. Paper no. TII-20-3561. (*Corresponding author: Kaiqi Sun.*)

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).

Kaiqi Sun and Weikang Wang are with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996 USA (e-mail: ksun8@utk.edu; wwang72@vols.utk.edu).

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

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/TII.2021.3063270>.

Digital Object Identifier 10.1109/TII.2021.3063270

**Index Terms**—False data injection attack (FDIA), high voltage direct current (HVdc) ancillary control, hybrid data-driven (HDD), multikernel support vector machine (MSVM).

## I. INTRODUCTION

HIGH voltage direct current (HVdc) systems have been successfully adopted as a solution to transmit bulk power over long distances and interconnect independent asynchronous power grids [1]. With the development of voltage source converter (VSC) technology, the functionality of the HVdc intertie has been significantly improved [2], [3].

An HVdc intertie has high controllability because it allows the independent control of active and reactive power, providing a quick dynamic response to various system disturbances. Therefore, the system configuration of HVdc intertie will result in benefits including reliability and ancillary-services [4]. In the result of interconnection seam study, the ancillary-services, including the frequency-response sharing, inertial response, and damping oscillation control, can provide 25% of the economic benefits using the HVdc intertie [4], [5]. Moreover, such economic benefits brought by the HVdc intertie assisted ancillary-services for ac grids are believed to offset the cost to construct the HVdc network [6].

Some power companies have tried applying the conventional HVdc interties for ancillary controls [7]–[9]. Specifically, the HVdc intertie utilizes real-time phasor measurement units (PMUs) feedback to construct a supplemental commanded power signal for the HVdc ancillary control. Based on the synchronization characteristic of the PMUs, in China, a wide-area adaptive damping control system through the modulations of multiple HVdc interties is developed by the china southern power grid [8]. In North America, a damping controller (DCON) utilizes a control scheme and real-time PMUs data to damp interarea oscillations by modulating the power, and has been implemented on the pacific dc intertie [9].

The performance of the ancillary service provided by the HVdc intertie is highly relevant to the accuracy of PMUs [10]. However, due to the fast power regulation capability of the HVdc intertie (power regulation rate could be up to 200 MW/s), the frequency deviation caused by false data injection attacks (FDIAs) may cause large power flow change of HVdc interties. For example, the impact of three types of cyberattacks on the HVdc transmission-based oscillation damping control was

studied, including the timing attack, replay attack, and FDIAs in [11]. The effect of attacks on the dynamic voltage stability and switching power losses and the vulnerabilities of the HVdc system is studied in work [12]. In the latest work [13], the vulnerability and impact of the hybrid ac/HVdc grid with virtual inertia to the FDIAs is also explored. The FDIA on the PMUs for the HVdc ancillary control may lead to the sever contingency in a system that is configured with HVdc interties [14]. Nowadays, with the growing probability of the FDIAs, the security of the PMU configured in the HVdc interties for ancillary control becomes a potential challenge to the system safety operation.

FDIA is a common type of data attack, which can happen on the communication and database levels [15]. Compared with bad data, the cyberattack is caused by the vulnerability of the network or communication protocol being exploited by the attacker [16]. However, most of the bad data are isolated and not in sequence [17]. And the number of contiguous bad data may no more than three points [18]. Based on the difference, bad data could be detected using some outlier detection methods or by setting the threshold. However, the FDIAs are different from bad data from another two aspects. 1) The attacked data may have no outliers. 2) The duration and amplitude of the attack can be maliciously modified to avoid outlier detection. Therefore, cyberattack can deceive the bad data detection [19]. For example, the synchrophasor data gradually changes in the form of a ramp, making it difficult to be found and managed [20]. To detect these FDIAs from PMU data, some research works have been conducted, which can mainly be categorized as model-driven and data-driven methods [15]. The model-driven method aims to establish a quasi-static or dynamic model to simulate power system parameters. Based on the real-time measurements, the weighted least squares and Kalman filter methods are introduced to detect the FDIA through the state estimation [21]. However, detection depends on the estimation method and system parameters. It means that the model-driven method may fail under an unknown model structure.

To address the limitations of the model-driven methods, some data-driven methods are proposed to detect FDIAs utilizing a data dependent and model-free manner. For example, the feed-forward artificial neural network (FANN) is developed to identify the spectrum of electric network frequency in [22]. Based on the study in [22], more than two methods are designed to distinguish data spoofing attacks including the multigrained cascade forest and random forest classification methods [23]. However, this article only considers the replacement of the frequency signal, which restricts its adaptability. Next, a discordant element approach is proposed to detect the FDIA in the dc microgrids [24]. Three attack numerical methods are simulated and verified. The above methods realize the identification of the attack, but the duration time of FDIA cannot be identified, which is an important control signal for the HVdc ancillary control. Therefore, using these methods, the performance of the HVdc ancillary control may be deteriorated.

To address these issues, this article proposes a hybrid data-driven (HDD) based HVdc ancillary control to improve the control performance of the HVdc interties under FDIAs. The contributions of this article are summarized as follows.

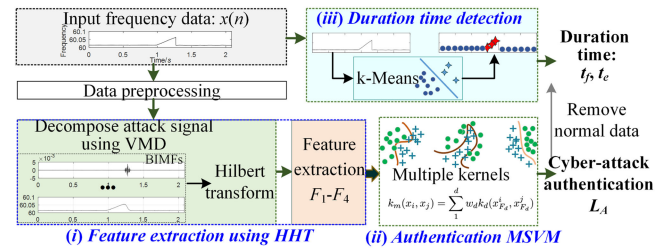


Fig. 1. Proposed HDD-based cyberattack detection framework.

- 1) To achieve automatic identification of multiple frequency attacks, the Hilbert Huang transform (HHT) is utilized to decompose the measurements into the band-limited mode functions (BMFs) with variational mode decomposition (VMD). Next, the Multikernel support vector machine (MSVM) is proposed to construct a novel form of kernels and automatically classifying different FDIAs.
- 2) Using the anomalous characteristics of attack data, the fast unsupervised learning method k-Means is used to obtain the duration time. An HDD framework is also proposed combined with the HHT, MSVM and k-Means. Instead of targeting a specific attack, features of multiple frequency data are fused and identified.
- 3) Benefiting from the fast classifying of FDIAs, an HDD-based HVdc ancillary control strategy is proposed to reduce the effect of the FDIAs on the HVdc intertie. Then, the system operation stability under FDIAs can then be guaranteed.

The rest of the article is organized as follows. The HDD detection framework of the multiple frequency attack is introduced in Section II. The steps for constructing the HDD are proposed in Section III. Then, the duration time detection is shown in Section IV. The HVdc ancillary control is presented in Section V. Different experiment results are shown in Section VI. Finally, Section VII concludes this article.

## II. DATA-DRIVEN BASED FDIA DETECTION FRAMEWORK

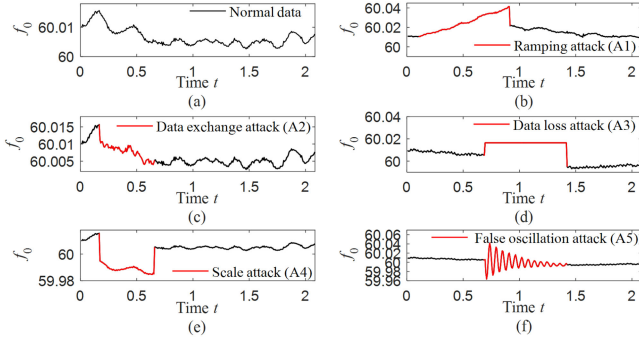
To accurately reduce the effect of the FDIA on the HVdc intertie, the cyberattack and duration time of the frequency data are detected first. Here, a novel hybrid data-driven base method with two objectives is proposed including classifying the attack and detecting its duration time, which including the start and end time. Denoting the measurement frequency data from the HVdc intertie as  $x(n)$ , the framework of the HDD cyberattack detection method is shown in Fig. 1. It consists of the following steps.

- 1) Feature extraction: The HHT is performed to decompose data  $x(n)$  and extract the features from the decomposition results.
- 2) Identification of FDIAs: Using the extracted features, a multikernel SVM method is proposed to classify different types of attacks and labeled as  $L_A$ .
- 3) Duration time detection: An unsupervised clustering method is used to identify the duration time of the attack. Combined with the identification results in the second

**TABLE I**  
FORMULATION OF ATTACK VECTORS

Different FDIAs ( $k_d$ )	Numerical models ( $k_d$ )
Ramping attack (A1)	$x(n) = x'(n) \pm \lambda_{ramp} t \Delta u(t)$
Data exchange attack (A2)	$x(n) = x'(n)(1 - \Delta u(t)) + x_1(n) \Delta u(t)$
Data loss attack (A3)	$x(n) = x'(n)(1 - \Delta u(t)) + f_{base} \Delta u(t)$
Scale attack (A4)	$x(n) = x'(n)(1 \pm \lambda_{scale} \Delta u(t))$
False oscillation attack (A5)	$x(n) = x'(n)(1 - \Delta u(t)) + \lambda_{osc} \Delta u(t)$

The  $u(t)$  is the heaviside step function.  $\Delta u(t) = u(t - t_1) - u(t - t_2)$ ,  $0 < t_2 - t_1 < S_t$ , where the  $t_1$  and  $t_2$  are the attack time.  $S_t$  is the sampling time of each FDIA.  $f_{base} = 60$  Hz, and different  $\lambda_x = \{\lambda_{ramp}, \lambda_{scale}\}$  is the magnitude of attack data.  $\lambda_{osc}$  is the false oscillation data.  $x_1(n)$  denotes the data from other measurement units.



**Fig. 2.** Five types of FDIAs.

step, the accuracy of duration time is optimized by excluding the normal frequency data. Finally, the detection results are fed to the HVdc control terminal.

In this article, five types of cyberattacks are considered including ramping attack (A1), data exchange attack (A2), data loss attack (A3), scale attack (A4), and false oscillation attack (A5). The numerical model and principle of these attacks are listed in **Table I** based on the definition in [20], [25]. The shapes of the attacks are shown in **Fig. 2**. Specifically, for the ramping attack, a gradual trend item is added to the measurement data  $x'(n)$ . And the magnitude of the attack data can be controlled by  $\lambda_{ramp}$  [20]. And it is challenging to distinguish between normal and A2 data as shown in **Fig. 2(a)** and **(c)** due to their similar shape. For the A3 and A4, it shows that higher or lower values are modified compared with the original measurement value. And the difference between A3 and A4 is that the A3 data are lost so the data  $f_{base} = 60$  Hz is compensated [25]. During  $t_1 = 0.7$  s and  $t_2 = 1.42$  s, it is clearly found that a false oscillation is added in A5, which may cause false control actions.

The duration and length of this FDIA can be modified arbitrarily. To bypass the bad data detection, the parameters of different FDIAs should meet certain mathematical conditions. Usually, the  $3\sigma$  criteria can be used to describe the characteristics of bad data [18]. The  $\mu$  is the mean value and  $\sigma$  is the standard deviation of the frequency data. If there is bad data, the bad data might be outside the range  $(\mu - 3\sigma, \mu + 3\sigma)$  [18]. According to this criterion, if the cyberattack would like to bypass the bad data detection, suitable threshold parameters and conditions can be set so that the characteristics of attacked data is located in between  $(\mu - 3\sigma, \mu + 3\sigma)$ .

Take the actual two-day measurement data from three PMUs (WECC system) as an example, the  $\mu$  and  $\sigma$  are 60, 60.0032, 59.9998 and 0.0138, 0.0139, 0.0139 Hz, respectively. The mean values of  $\mu$  and  $\sigma$  can be set to 60.001 and 0.01386 Hz, respectively. This means that the measurement frequency value outside the (59.95942, 60.04258) Hz can be treated as bad data.

For the ramping attack, the magnitude  $\lambda_{ramp} t$  will determine whether the A1 can pass the bad data detection. Here, the  $x'(n)$  is set to 60 Hz, the  $\lambda_{ramp} t$  should be satisfied  $\lambda_{ramp} t + x'(n) \in (59.95942, 60.04258)$  Hz, and therefore the  $\lambda_{ramp} t$  be located between -0.04258 and 0.04058 Hz. For the data exchange attack, the data is similar to the raw data, thus the magnitude will not exceed the range of  $(\mu - 3\sigma, \mu + 3\sigma)$ . For the data loss attack, the  $f_{base} = 60$  Hz is compensated for A3. Obviously, this data range is the normal range. For the scaling attack, the  $\lambda_{scale}$  determines the magnitude and it should be satisfied  $x'(n)(1 \pm \lambda_{scale}) \in (59.95942, 60.04258)$  Hz, and therefore  $\lambda_{scale}$  can be located in (-0.04258, 0.04058) mathematically. Otherwise, the A4 can be detected by the bad data detection. For the false oscillation attack, it also will bypass the bad data detection only if the amplitude and duration of the false oscillation coincide with the real event. The attackers can collect some historical events to forge a false oscillation attack.

### III. IDENTIFICATION OF MULTIPLE FREQUENCY DATA

#### A. Signal Decomposition for FDIA Data

The first step to identify the cyberattack is to extract the deterministic features. The HHT is a nonlinear signal processing method that includes EMD and Hilbert transform (HT). It is suitable for processing nonlinear signals. Compared with the S transform [26], the HHT consumes less calculation time because the S transform needs to calculate multiple FFTs. However, the empirical mode decomposition (EMD) is prone to fall into modal aliasing, which leads to spectrum overlapping of frequency data. Then the ensemble EMD (EEMD) is proposed as an improved method based on EMD. However, EEMD usually integrates a large number of EMD calculation results and therefore increases the amount of calculation. To mitigate this problem, a frequency bandwidth decomposition method named VMD is used to replace the EMD process during the calculation of HHT. Compared with the EMD, the modal aliasing and endpoint effect problem of VMD can be mitigated when decomposing a nonlinear signal [27].

The purpose of VMD is to decompose the frequency data as  $x(n)$  into a combination of different BMFs  $b_t(n)$  [27]. Each BMFs has a center frequency  $\omega_t$ , where the  $t$  denotes the number of BMFs. The primary principle of VMD is to solve a constrained variational problem, which can be expressed as

$$\min_{\{b_t\}, \{\omega_t\}} \left\{ \sum_t \left\| \frac{\partial}{\partial t} \left[ \left( \delta(t) + \frac{j}{\pi n} \right) * b_t(n) \right] \exp^{-j\omega_t n} \right\|_2^2 \right\}$$

$$\text{s.t. } \sum_t b_t(n) = x(n)$$
(1)



where  $\delta(t)$  and  $*$  sign denote the Dirac distribution and convolution operation respectively. The frequency shift factor  $\exp^{-j\omega_t n}$  is used to adjust the center frequency  $\omega_t$  to the predicted center frequency.

To address the variational problem, the quadratic penalty term and Lagrange multiplier are introduced. Using the alternative direction method of multiplier (ADMM), the center frequency  $\omega_t$  and BMFs  $b_t(n)$  can be constantly updated. Then the output of VMD can be expressed as

$$x(n) = \sum_1^{t-1} b_t(n) + b_{tr}(n) \quad (2)$$

where the  $b_{tr}(n)$  is the residual mode component. Commonly, the  $b_{tr}(n)$  represents the changing trend of the frequency data.

After obtaining the BMFs of FDIA, the physical parameters including the magnitude and frequency of each BMFs can be calculated according to the HT. Specifically, the BMFs is transformed into an analytic function by adding the imaginary part. This analytic function  $H_b(n)$  can then be obtained as

$$H_b(n) = b_t(n) + j\bar{b}_t(n) \quad (3)$$

$$b_t(n) + j \frac{c_a}{\pi} \int_{-\infty}^{+\infty} \frac{b_t(\tau)}{n - \tau} d\tau$$

where the  $c_a$  indicates the Cauchy principal value,  $\bar{b}_t(n)$  is the imaginary part of  $b_t(n)$ . Thereafter, the magnitude, phase and frequency of each BMFs can be derived from (3).

## B. Feature Extraction

Once the BMFs of frequency data are decomposed, the next step is to extract the features so that the FDIA data can be easily detected. As can be seen from HHT, the sources of features can be inferred from the results of VMD and HT. The motivation of feature selection is to extract as many types of features as possible and avoid increasing the amount of calculation. The initial feature selection process is performed to filter out some redundant and low-precision features.

Accordingly, four distinctive features  $F_1 - F_4$  are designed from HHT. These four features can be divided into two groups including two frequency domains and another two statistical features. The first  $F_1$  is the primary frequency point of each BMFs which is derived from the instantaneous frequency [28]. The computation of the instantaneous frequency can be referred to [29]. The second  $F_2$  is the amplitude spectrum of frequency data with the trend term removed. The spatial and temporal characteristics of synchronized data are different if the measurement data comes from different regions [23]. Therefore, the frequency properties will be changed if the data is attacked. The definition of  $F_1$  [29] and  $F_2$  are as follows:

$$F_1 = \frac{1}{2\pi n} \sum_n \frac{d}{dn} \arctan \frac{\bar{b}_t(n)}{b_t(n)} \quad (4)$$

$$F_2 = \sum_{n=0}^{N-1} (x(n) - b_{tr}(n)) e^{(-i2\pi kn)/N}, k = 0, \dots, N-1 \quad (5)$$

where  $N$  is the length of the frequency data  $x(n)$ . In  $F_2$ , the trend item  $b_{tr}(n)$  is removed from  $x(n)$ . The reason is that some attackers will replace the frequency data between multiple PMUs, while retaining the synchronous changes of the data. In this case, the recognition accuracy will be interfered if the trend item is retained.

Another two statistical features are the kurtosis ( $F_3$ ) and envelope entropy ( $F_4$ ). The definition of  $F_3$  and  $F_4$  can be expressed as [30]

$$F_3 = E \left[ \left( \frac{b_t(n) - \mu_b}{\sigma_b} \right)^4 \right] \quad (6)$$

where  $\mu_b$  is the mean value of each BMF, and  $\sigma_b$  is the standard deviation of BMF. The  $F_3$  describes the shape of the BMFs, thus it has the potential to identify different attacks.

The definition of  $F_4$  is [31]

$$F_4 = \sum_{j=1}^{s_t} \left( a(j) / \sum_{j=1}^{s_t} a(j) \right) \log \left( a(j) / \sum_{j=1}^{s_t} a(j) \right) \quad (7)$$

where  $a(j)$  denotes the envelope of the Hilbert transfer of  $b_t(n)$ , the  $s_t$  is the length of each BMF. The purpose of using envelope entropy is to measure the signal irregularity such as sparse characteristics.

## C. Frequency Data Identification Using MSVM

To improve the detection performance, the SVM is used as the primary classification method which is a supervised process. Generally, the form of kernel function is relatively simple and fixed because one kernel function is used to process the input vector. Hence, SVM is difficult to apply to identify complex FDIAs, especially when the system is multi-input. To solve this limitation, a multikernel SVM is proposed to improve its FDIA detection capabilities.

Given the feature dataset  $D = (F_d, y_x)$ ,  $d = 1, 2, 3, 4$ , where the  $y_x$  is the label of  $F_d$ . The motivation of MSVM is to learn a hyperplane to separate the  $F_d$ . In MSVM, the purpose of the kernel function is to map the  $F_d$  to different hyperplanes. These indistinguishable input vectors can then be separated from each other after mapping. Some most commonly used kernels are the linear kernel, polynomial kernel, sigmoid kernel, and radial basis function (RBF) kernel. For instance, the RBF can be defined as

$$k_r(x_i, x_j) = \exp \left( -\frac{\|x_i - x_j\|_2^2}{2\sigma_k^2} \right) \quad (8)$$

where  $x_i, x_j \in x(n)$ ,  $\sigma_k$  indicates the width kernel parameter for adjusting the kernel shape.

In SVM, only a single kernel and a fixed parameter is used which limits the learning ability when processing the cyberattack data. However, not all features contain equal effective information. Considering the unequal information for different features, a multikernel methodology is proposed in MSVM, which the

definition can be expressed as

$$k_m(x_i, x_j) = \sum_1^d w_d k_d(x_{F_d}^i, x_{F_d}^j)$$

$$\text{s.t. } \sum_1^d w_d = 1, d = 1, 2, 3, 4 \quad (9)$$

where the  $k_d(x_{F_d}^i, x_{F_d}^j)$  denotes corresponding kernel functions of input feature  $F_1 - F_4$ .  $w_d$  denotes the weight of kernel  $k_d$ , it is used to adjust the proportion of different features. Basically, the  $k_m$  is a linear combination of multiple kernel functions. Different from the SVM, multiple kernels are used to increase flexibility. Meanwhile, each input feature of FDIA can be mapped by a single kernel function. Therefore, it is expected to obtain four suitable kernel functions and parameters for  $F_1 - F_4$ .

After that, an objective function is established to learn the decision boundary  $\Theta : \omega^T k_m(x_i, x_j) + b = 0$ , which can be written as [32]

$$\min(\omega, \xi_i) = \frac{1}{2} \|\omega\|^2 + C \sum_{i=1}^n \xi_i \quad (10)$$

$$\begin{cases} \text{s.t. } y_x(\omega, k_m(x_i, x_j)) + b \geq 1 - \xi_i \\ \xi_i \geq 0, i = 1, \dots, n \end{cases} \quad (11)$$

where the  $\omega$  and  $b$  are the weight and bias value of learning decision boundary, respectively,  $\xi_i$  is the slack variable,  $C$  denotes the regularization parameter.

This objective function can be solved by introducing the Lagrange multipliers. The labels of unknown attacked frequency data can be predicted ( $L_A$ ) utilizing the decision boundary. To achieve sufficient performance, the parameters of MSVM (such as  $C, \sigma_k$ ) need to be tuned during the training process.

#### IV. DURATION TIME DETECTION FOR FDIA DATA

In the previous step, when the attack just ends, the frequency data may still be marked as an attack signal by MSVM because this data still contains a small piece of tampered data. Therefore, the detection of duration time helps to improve the real-time control in HVdc intertie once the attack disappears.

The duration time detection of false frequency injection consists of the start and end time detection. Essentially, the duration time detection is a binary classification, where each attack data point is divided into normal and abnormal data. Here, the unsupervised k-Means cluster method is used to separate FDIA data. The advantage of k-Means is that its detection speed is fast, and the number of clustering categories can be specified.

The objective of k-Means is to partition the frequency data into  $\eta$  clusters. For each cluster, there is an adaptively changing cluster centroid. Denoted the cluster subsets and corresponding cluster centroid as  $C_i$  and  $c_i$ , respectively. The  $x_n$  indicates the  $n$ th data point of  $C_i$ . Typically, the determination of the cluster center includes the following steps [33].

- 1) *Step 1*: Initialize  $\eta$  cluster centroid  $c_i$  using the random method. The number of clusters  $\eta$  is set to 2, which represents the normal and attacked clusters.

- 2) *Step 2*: For the cluster center  $c_i$ , select the  $x_n$  and determine which  $c_i$  is closest to  $x_n$ . These  $x_n$  close to  $c_i$  are regarded as a cluster  $C_i$ .
- 3) *Step 3*: Calculate the mean value of each cluster  $C_i$  in step 2, and then move the cluster center  $c_i$  to the location of the mean value.
- 4) *Step 4*: Repeat steps 1 to 3 until the cluster center  $c_i$  no longer changes.

After that, the frequency data point in one cluster  $C_i$  belongs to the same cluster. For example, if the  $x_n$  in  $C_1$  is the normal cluster, then the rest of the data in  $C_2$  means the attacked data. The duration time can then be obtained by counting the location and length of the attacked data. In the interval of FDIA, multiple consecutive detected attack data points are identified as the beginning and the end of FDIA, which are denoted as  $t_f$  and  $t_e$ . The  $t_e$  means that HVdc can reuse the measured frequency data as soon as the attack disappears.

To evaluate the detection effect of the duration time, a mean accuracy (MA) evaluation index is proposed as

$$MA = \frac{1}{\eta} \sum_i \frac{x_i}{L_x}, i = 1, 2 \quad (12)$$

where  $x_i$  denotes the number of correctly identified data points in  $i$ th cluster,  $L_x$  denotes the length of the frequency data.

#### V. HDD-BASED HVDC ANCILLARY CONTROL

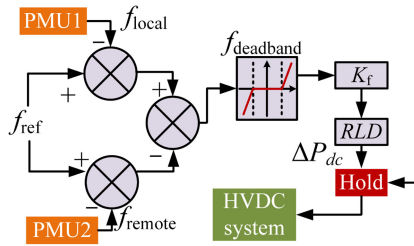
With the proposed HDD, the types and duration time of the attacked frequency data could be obtained. It provides an opportunity for the HVdc intertie operator to classify the events with a small delay. Then the preventive control strategies can be adopted to reduce the influence caused by cyberattack on HVdc ancillary control.

Here, an HDD-based HVdc ancillary control is proposed for suppressing the effect of the FDIA to the HVdc intertie. The HDD-based HVdc ancillary control consists of two control functions: detection-period ancillary control function (DACF) and cyberattack response control function (CRCF).

The objective of the proposed DACF is to provide an appropriate ancillary control to respond to the system disturbance in a certain while keeping its response capacity for avoiding potential cyberattack. The control diagram of the DACF is shown in Fig. 3.

As shown in Fig. 3, when the frequency deviation ( $f_{\text{ref}} - f_{\text{local}}(f_{\text{remote}})$ ) is over the  $f_{\text{deadband}}$ , the DACF is activated. The DACF generates a  $\Delta P_{\text{dc}}$  by calculating the deviation between the nominal and operating frequency. Then  $\Delta P_{\text{dc}}$  is sent to the power control terminal to adjust the power flow on the HVdc intertie. The working period of the DACF is from the beginning of the event until the HDD detects the type and duration time of the cyberattack. Different from the conventional frequency response control, the droop coefficient  $K_f$  in the DACF adopts a smaller value. Although this  $K_f$  selection may lose part of the frequency response capability of the HVdc intertie at the beginning of the event but could avoid the significant influence caused by cyberattack.

After that, the ancillary control of the HVdc intertie is achieved through the proposed CRCF. The objective of CRCF is



**Fig. 3.** Control diagram of the detection-period ancillary control function, where RLD is the rate limiter dynamic in order to avoid the power output pulse of the HVdc ancillary control,  $f_{local}$  is the operating frequency monitored at PCC bus of power control terminal,  $f_{remote}$  is the operating frequency monitored at PCC bus of dc voltage control terminal, the  $f_{ref}$  is the nominal frequency,  $f_{deadband}$  is the dead-band of the FPDC,  $K_f$  is the droop coefficient of the detection-period ancillary control and  $\Delta P_{dc}$  is power adjustment of the HVdc intertie.

to provide fast and adequate ancillary control after getting the results from HDD. Therefore, the insufficient response caused by DACF and the influence caused by FDIAs can be compensated. The general control diagram of the HDD-based HVdc ancillary control is shown in Fig. 4.

As shown in Fig. 4, the CRCF could be divided into two stages. Five types of cyber-attack methods (A1–A5) can lead to three potential wrong operating situations of the ancillary control of the HVdc intertie—triggering fake event, burying real event, and inverse response event. Thus, the stage I of the CRCF is to classify the detected FDIA into three types. This distinction is based on the following considerations.

- 1) The A1, A3, A4, and A5 can fake an event to the HVdc intertie, such as a generator trip event or load trip event, and the HVdc intertie may be misleading and provide wrong ancillary control to its connected ac system.
- 2) Besides the triggering fake event, the A3 can also cause HVdc intertie to not provide the ancillary control during the system event.
- 3) Among the attack methods A1–A5, the A2 has the worst potential effect on the ancillary control of the HVdc intertie. The A2 may lead to the HVdc intertie provide inverse ancillary control to the disturbed system, which further exacerbates the influence of the system event.

After that, stage II of the CRCF is to develop four control strategies for suppressing the influence caused by the FDIAs, including normal strategy, the fake event recovering strategy, fast recovering strategy, and fast reversal strategy.

The normal strategy is designed for the ancillary control adjustment of the HVdc intertie when no FDIA happens based on the results from HDD. Due to the control delay caused by HDD calculation, the CRCF needs to compensate for the response insufficient of DACF. The normal operation strategy of the CRCF is to adjust the  $K_f$  of DACF to  $K_{normal}$  to provide faster ancillary control, so that similar ancillary control performance with conventional HVdc ancillary control can be realized.

The fake event recovering strategy aims at recovering the wrong ancillary control. When the label  $L_A$  of FDIAs is detected by HDD and the HVdc intertie has been providing ancillary control to the system due to the fake event signal, the fake event

recovering strategy is activated. The control process of the fake event recovering strategy can be described as follows.

- 1) *Step 1:* The CRCF sends a signal to the *hold* function in the DACF to stop the further ancillary control from the DACF.
- 2) *Step 2:* The CRCF adjusts the current power flow of the HVdc intertie back to the original power flow.
- 3) *Step 3:* Release the *hold* function in DACF in order to eliminate the influence caused by the cyberattack.

To compensate for the response blocking of the HVdc intertie during the event, the objective of the fast recovering strategy is to provide the fastest response using the HVdc intertie in the disturbed system. When the FDIA is detected by HDD and the buried real event is redetected at  $t_f$ , the CRCF adjusts the  $K_f$  of DACF to  $K_{f-max}$  so that providing ancillary support to the disturbed system as much as possible.

The fast reversal strategy is developed to mitigate the effect of the inverse response event. When the cyber attack is detected by HDD and the HVdc intertie is providing the inverse ancillary control, the control process of the fast reversal strategy could be described as follows.

- 1) *Step 1:* The fast reversal strategy of the CRCF exchanges the measured data from PMUs in the DACF.
- 2) *Step 2:* The CRCF adjusts the  $K_f$  of DACF to  $K_{f-max}$  so that providing correct ancillary control with the maximum response rate. The disturbance caused by the event and inverse HVdc ancillary control can then be suppressed until the end time of the cyberattack.

## VI. EXPERIMENTS AND ANALYSIS

### A. Comparison of Different Attack Intensity and Duration Time

To verify the control performance of HVdc under cyberattack, two types of experiments are conducted, including the HDD-based FDIA detection and HDD-based HVdc control performance experiments.

The first experiment is to verify the performance of the HDD. Specifically, the high-speed sampling frequency data with 1440 Hz reporting rate is collected in the Eastern Interconnection system. Totally 18 000 samples are used, wherein the length of each sample is 4500. All the samples are divided into three parts including the training, verification and test set. Moreover, reserved PMU data that did not participate in training is used to verify the data exchange attack. In HDD, the parameters of MSVM is optimized by the particle swarm optimization (PSO) method. To achieve real-time detection, the input frequency data is downsampled to 500 points per sample and then the feature  $F_2$  is downsampled to 25 points.

The characteristics of the attack determine the response behavior of the HVdc control system. In this section, two characteristics including attack intensity and duration time are considered to verify the effectiveness of the HVdc control. The kernels have a great impact on the MSVM, thus different kernels are first evaluated. The attack identification results under some commonly used kernels are listed in Table II.

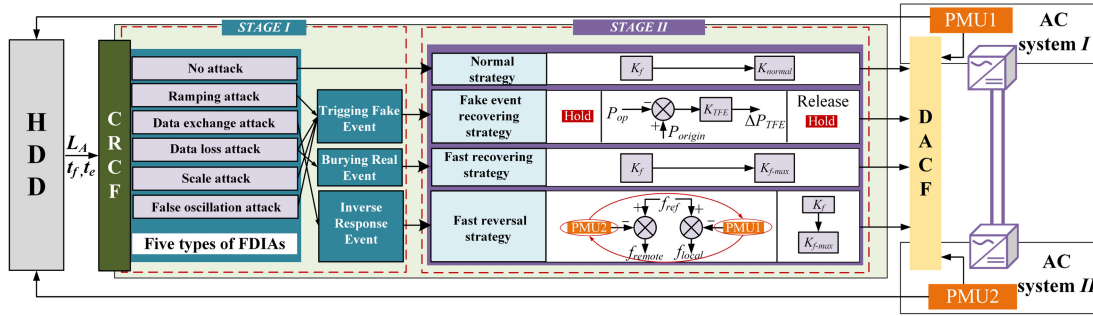


Fig. 4. Control diagram of the proposed HDD-based HVdc ancillary control, where  $K_{normal}$  is the droop coefficient of CRCF normal strategy,  $P_{op}$  is operating power flow of the HVdc intertie,  $P_{origin}$  is the power flow of the HVdc intertie before the cyberattack, the  $\Delta P_{TFE}$  is power output of the CRCF fake event recovering strategy, the  $K_{f-max}$  is the maximum droop coefficient of the HDD-based HVdc ancillary control.

TABLE II  
PERFORMANCE USING DIFFERENT MULTIKERNEL SVM

Multi-kernels ( $k_d$ )				Accuracy (%)
$k_1$	$k_2$	$k_3$	$k_4$	
Lin	Lin	Lin	Lin	92.03
Pol	Pol	Pol	Pol	93.85
Pol	Pol	Lin	Lin	93.72
RBF	RBF	RBF	RBF	94.28
Pol	Pol	RBF	RBF	<b>94.98</b>

TABLE III  
PERFORMANCE COMPARISON UNDER DIFFERENT ATTACK INTENSITY

Models	Accuracy (%)			Test time (ms)
	50 mHz	100 mHz	200 mHz	
HHT(EEMD)-MSVM	86.85	86.78	87.09	40.16
HHT(VMD)-SVM	92.71	92.18	92.56	37.75
HHT(EWT)-MSVM	83.11	85.28	84.92	<b>0.75</b>
HHT <sub>1</sub> (VMD-no $F_1$ )-MSVM	94.17	93.56	94.43	38.46
<b>HHT(VMD)-MSVM</b>	<b>95.30</b>	<b>94.19</b>	<b>95.45</b>	38.73

It is worth noting that the optimized weight  $w_d$  and kernel parameters are used in the following experiments. The bold entities mean that this method has higher accuracy. It can be seen from Table II that the HDD obtains the lowest accuracy when all the kernels are linear kernels. Generally, the RBF kernels have better performance. After combining the polynomial and RBF kernels, 94.73% accuracy is achieved. Finally, the weights  $w_d$  are set to  $\{0.0561, 0.4430, 0.3450, 0.1559\}$ . The kernel parameters of  $k_d$  are set to  $\{6.0820, 2.8592, 8.5668, 0.9307\}$ . Meanwhile, the number of BMFs is set to  $t = 6$  using the grid search method.

Next, different attack intensity experiments are used to verify the results of the proposed HHT-MSVM. The attack intensity means the amplitude difference before and after the attack. The empirical wavelet transform (EWT) [34] and EEMD are used to compare with the VMD. The attack identification results are listed in Table III. The test time is the running time per sample. To verify the effectiveness of this feature  $F_1$ , an experiment that does not contain this feature is conducted. The HHT<sub>1</sub> denotes the weight of  $F_1$  is assigned to  $F_3$  (weight of  $F_3$  becomes  $w_3 = 0.4011$ ). The other parameters of HHT<sub>1</sub>(VMD-no  $F_1$ )-MSVM are the same as the HHT(VMD)-MSVM. For a fair comparison and to ensure that the dimensions of features are consistent, the number of decomposition is set to 6 for both EWT and EEMD.

The vector of initial bounds is set to  $[2, 50, 100, 150, 200]$  where the adaptive regression method is used in the EWT method.

Compared with HHT-MSVM using EEMD and VMD, the results show that the HHT with VMD performs better than the EEMD method. This is because the VMD is suitable for the decomposition of nonlinear signals. Compared to EWT and VMD methods, it can be seen that the results of EWT-MSVM is about 85% and is lower than the accuracy of EEMD and VMD under different attack intensity. This reason is that the filter is used in EWT, and the filter causes energy leakage, which introduces decomposition errors. The other reason is that the features extracted by the decomposition result of EWT are not distinguishable. Additionally, the proposed MSVM obtains about 2.7% higher than the SVM method under different attack intensities. Compared with HHT<sub>1</sub>(VMD-no  $F_1$ )-MSVM and HHT(VMD)-MSVM, the results show that the  $F_1$  contributes to the improvement of identification accuracy for FDIAs, which more than 1% accuracy can be improved. The EEMD-MSVM consumes more time than because the EEMD is derived from multiple EMD calculations. However, the detected speed of EWT is the fastest one, which indicates the EWT has the best real-time performance. Meanwhile, the running time of MSVM is similar to SVM, which indicates the effectiveness of MSVM.

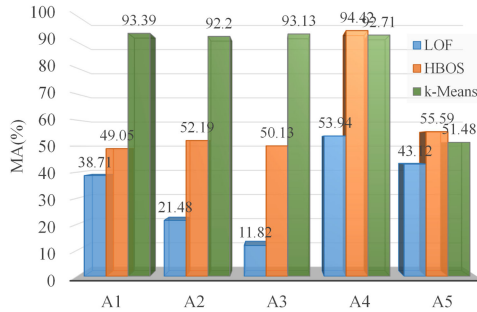
To compare the performance of MSVM with other classifiers, three types of commonly used classifier methods are selected, including the random forest (RF) and artificial neural network (ANN), and ridge classifiers [35]. For the RF, the max depth parameter is optimized set to 12 from [1, 15]. For ANN, the structure is set as 43-40-30-6, which the 43 and 6 denotes the input features and output classes, respectively. The number of hidden nodes are 40 and 30, which is selected through trial and error. The regularization strength parameter of the Ridge classifier is set to 0.5 through the grid search method. The  $F_1$  and  $F_4$  features are connected together and fed into different classifier methods. The identification results are listed in Table IV.

As shown in Table IV, it can be seen that the ANN and Ridge have similar performance and test time for FDIAs. The maximum 86.11% is obtained for ANN and Ridge classifiers, indicating the weaker ability to identify different FDIAs. The highest performance of RF is 95.13%, which means that the RF has high recognition ability. Compared with RF and MSVM, the MSVM obtains 1% higher accuracy than the RF with 100 mHz attack intensity. This means that the MSVM has better



**TABLE IV**  
PERFORMANCE COMPARISON UNDER DIFFERENT  
CLASSIFICATION METHODS

Models	Accuracy (%)			Test time (ms)
	50 mHz	100 mHz	200 mHz	
HHT(VMD)-RF	94.90	93.14	95.13	38.49
HHT(VMD)-ANN	80.04	80.31	82.94	<b>38.48</b>
HHT(VMD)-Ridge	85.92	85.35	86.11	<b>38.48</b>
<b>HHT(VMD)-MSVM</b>	<b>95.30</b>	<b>94.19</b>	<b>95.45</b>	38.73



**Fig. 5.** Comparison of three duration time detection methods.

**TABLE V**  
PERFORMANCE COMPARISON USING DIFFERENT DETECTION METHODS

Models	Accuracy (%)			MA(%)	Test time (ms)
	30%	40%	50%		
CNN	75.96	76.59	81.66	-	$9 \times 10^{-2}$
CNN-LSTM	83.36	84.15	85.44	-	0.23
WT-FFT-ANN	74.51	74.93	76.22	-	5.35
<b>HDD</b>	<b>94.61</b>	<b>94.89</b>	<b>95.30</b>	<b>84.58</b>	57.78

-: the method cannot achieve duration time detection.

performance because multiple kernel functions are used. The detection time of different methods is less than 39 ms, which reveals that these classifiers have similar computational efficiency. Overall, the effectiveness of the proposed HHT-MSVM is verified compared with different decomposition methods and classifiers.

To compare the accuracy of the k-Means and some advanced unsupervised method, the duration time result is further carried out as presented in Fig. 5. The local outlier factor (LOF) and histogram-based outlier detection (HBOS) are two fast outlier detection methods [36]. In these three methods, the cluster parameter can be set as 2 to classify the normal and attack data points. The minkowski distance is used in LOF. And the amount of contamination is set to 0.1 in LOF and HBOS. The results depict that the k-Means has higher MA values than the LOF and HBOS for A1-A4. The accuracy of A5 is relatively low is because the attacked data value is very closed to the normal data. Eventually, most of the cyberattack methods can be detected by the k-Means.

### B. Comparison With State-of-the-Art Methods

Thereafter, three advanced frequency data detection methods are used to further verify the performance under different ratios of training data, as shown in Table V. These methods include the convolutional neural network (CNN), long short-term memory

**TABLE VI**  
PERFORMANCE COMPARISON USING STATE-OF-THE-ART METHODS

Models	Accuracy (%)			MA(%)	Test time (ms)
	30%	40%	50%		
MM-RFC	72.86	73.02	73.58	-	<b>1.93</b>
MM-gcForest	63.45	64.24	66.47	-	2.21
EEMD-FFT-BP	72.84	73.07	72.95	-	43.25
<b>HDD</b>	<b>94.61</b>	<b>94.89</b>	<b>95.30</b>	<b>84.58</b>	57.78

-: the method cannot achieve duration time detection.

(CNN-LSTM), and WT-FFT-ANN [22]. Both CNN and CNN-LSTM can automatically extract and identify the features from the input frequency data. It demonstrates that the accuracy of CNN and WT-FFT-ANN are the lowest, which only 76.22% and 81.66% accuracy are obtained under 50% training data. This is because CNN does not learn frequency domain features due to limited input information. The HDD has a profound performance in which 94.61% accuracy is reached even with 30% training data. Compared with WT-FFT-ANN, the HDD receives rich input features, including frequency and statistical domain. The test time of HDD is 57.78 ms, which the real-time HVdc ancillary control can be satisfied.

To compare the proposed method with some state-of-the-art FDIA detection methods, three state-of-the-art methods are selected, including the mathematical morphology (MM)-random forest classification (RFC) [37], MM-gcForest [23], and EEMD, fast Fourier transform (FFT), and back propagation (BP) neural network [38]. For the method MM-RFC [37] and MM-gcForest [23], the MM is used to decompose the extracted FDIAs, and then 62 features (sparsity trends and sparsity roughness features) are extracted from the results of MM. Finally, the feature is fed into the classifiers. For the EEMD-FFT-BP method, all the frequency domain features are extracted using EEMD and FFT. To achieve a fair comparison, the number of decomposed intrinsic mode functions of EEMD is also set to 6. The length of the input features for BP is 1500. A two-layer BP is used and the nodes of each layer are 200 and 100. The detection results are listed in Table VI.

It can be seen that the MM-gcForest and MM-RFC obtain lower accuracy, where the accuracies under different training data are less than 75%. However, the EEMD-FFT-BP has a higher performance than the MM-RFC. This reason is that more features are retained (1500 points for the input). However, only two types of features are extracted for MM-gcForest and MM-RFC, which means these two types of features can not fully characterize the FDIAs. The HDD obtains higher accuracy because four features from the frequency domain and statistics domain are used. This means more information is retained. However, the test time of HDD is also longer because it takes time to determine the attack time and VMD calculation.

The message authentication scheme (MAC) is mainly used in the advanced metering infrastructure (AMI), where the smart meters are the primary devices [39]. MAC also has the potential to be used in a wide-area measurement system (WAMS). To compare the proposed HDD with the lightweight MAC method, the comparison results from the security perspective and computational requirements' perspective can be summarized in Table VII.



**TABLE VII**  
COMPARISON OF THE PROPOSED HDD AND MAC METHODS

Index	HDD	MAC
Security for FDIA	Protected	Protected
Computational requirements	57.78ms	2000-bit, 180us [40] 200000-bit, 3000us [41]
Differences	CPU needed(real time) Based on IEEE C37.118, IEC 61850-90-5 [42]	CPU needed(real time) [41] Hash-based MAC or A-codes [40]

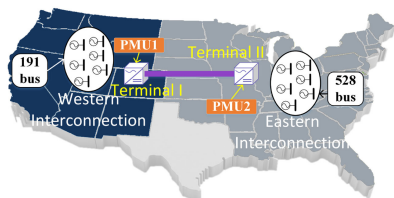


Fig. 6. Configuration of the two-terminal VSC-HVdc intertie system.

It can be seen that both the proposed HDD and MAC can defend the FDIA. For the MAC, take the Hash-based message authentication code (HMAC) as an example, if the message length is 2000-b, the worst execution time of HMAC is about 180 us [40]. And when the number of message length increases to 200 000 b, the verification delay would be 3000 us [41]. It can be seen that the proposed HDD and MAC can meet the real-time performance, where the MAC is faster.

It should be noted that there are some differences between the HDD method and MAC. The data-driven HDD method is based on the vulnerability of the transmission protocol. The purpose is to detect attack class and the duration time once the attack has occurred. The MAC is a type of cryptographic protection scheme, where its main purpose is to prevent being attacked. The HDD method can be deployed in a data server of the WAMS or a controller center. The MAC requires the meter to generate the key and encapsulate it in the security header of the data packet [43]. Therefore, the MAC needs to deploy distributed at each measuring device and data server.

### C. Verification of HDD-Based HVDC Ancillary Control

The second experiment is to verify the effectiveness of the proposed HDD-based HVdc ancillary control. An integrated North American power system model is developed in PSCAD simulation software by combining the highly reduced models of EI and WECC, using two-terminal VSC-HVdc intertie between the interconnections, as shown in Fig. 6.

The highly reduced models of EI and WECC are developed based on a reduced equivalent system, which the data can be found in [44]. This reduced equivalent system has been verified from the frequency response perspective. To realize the effective PSCAD modeling, highly reduced models of EI and WECC are redesigned using the 7 and 6 dynamic cluster generations, which is further reduced from the reduced equivalent system in [44]. The corresponding dynamic cluster generation capacity can be referred to [4]. Combined with Fig. 6, the terminal I works at constant dc voltage control, and the terminal II works at constant power control in HVdc intertie. The HDD-based

**TABLE VIII**  
QUANTIFY COMPARISON OF HVDC FREQUENCY REGULATION CONTROL

Index	A1		A3		A2	
	No HDD	HDD	No HDD	HDD	No HDD	HDD
$D_l$	0.129	0.081	0.226	0.121	0.167	0.163
$D_a$	0.073	0.012	0.105	0.017	0.063	0.006

HVdc ancillary control is configured on the terminal I to provide power support under the event.

In this section, three different types of FDIA are selected to verify the performance of the proposed HDD-based HVdc ancillary control including A1, A2, and A3. Fig. 7 shows the performance of HDD-based HVdc ancillary control under different types of frequency data attacks. Here, the ramping attack case is taken as an example and described in detail. It is notable that the purple star in Fig. 7 denotes the  $t_f$ .

As shown in Fig. 7(a1), a ramping attack with 0.7 Hz magnitude injects into PMU1 at 3 s. The HVdc intertie detects the frequency change from the PMU1 data and starts to activate its HVdc ancillary control. The power flow on the HVdc intertie from the PMU1 system to the PMU2 system is increased. Due to the power injection from the HVdc intertie, the frequency in the PMU2 system is also increased.

Without HDD-based HVdc ancillary control, due to the wrong response from the traditional HVdc ancillary control, the frequency measurement of PMU2 continuously deviates from the normal frequency as shown in Fig. 7(a2) and 7(a3). The largest frequency deviation of PMU2 reached 0.20 Hz. The power flow on the HVdc intertie also deviates from scheduled power, the largest power deviation is about 350 MW. However, with the HDD-based HVdc ancillary control, the FDIA is detected at  $t_f = 5.1 s$ , then the label  $L_A$  and  $t_f$  is sent to CRCF of HVdc intertie. The CRCF is activated and an appropriate control strategy is selected according to label  $L_A$ . Then the control signal is sent from CRCF to DACF and the power flow from PMU1 system to PMU2 system is decreased speedily. In Fig. 7(a2) and (a3), it shows that the frequency and power flow start to recover and back to the nominal value under the HDD-based HVdc ancillary control. From the solid blue line of Fig. 7(a2) and (a3), the largest frequency deviation and power deviations are less than 0.02 Hz and 50 MW, which has been significantly reduced after 13 s.

Combing the results from Fig. 7(b) and (c), it is clearly found that the HDD-based HVdc ancillary control could significantly suppress the frequency oscillation and realize the fast frequency recovery. Besides, to quantify the HVdc ancillary control performance, two indexes, including the largest frequency deviation ( $D_l$ ) and average frequency deviation ( $D_a$ ) are adopted as the indexes to quantify the HVdc ancillary control performance. Table VIII shows the quantified comparison of the HVdc ancillary control performance with and without the HDD methods. As shown in Table VIII, both the largest frequency deviation and average frequency deviation of the HVdc ancillary control with HDD is much smaller than the HVdc ancillary control without HDD. Overall, the performance of HDD-based HVdc ancillary control indicates that the active power and frequency are adjusted accurately and in time.

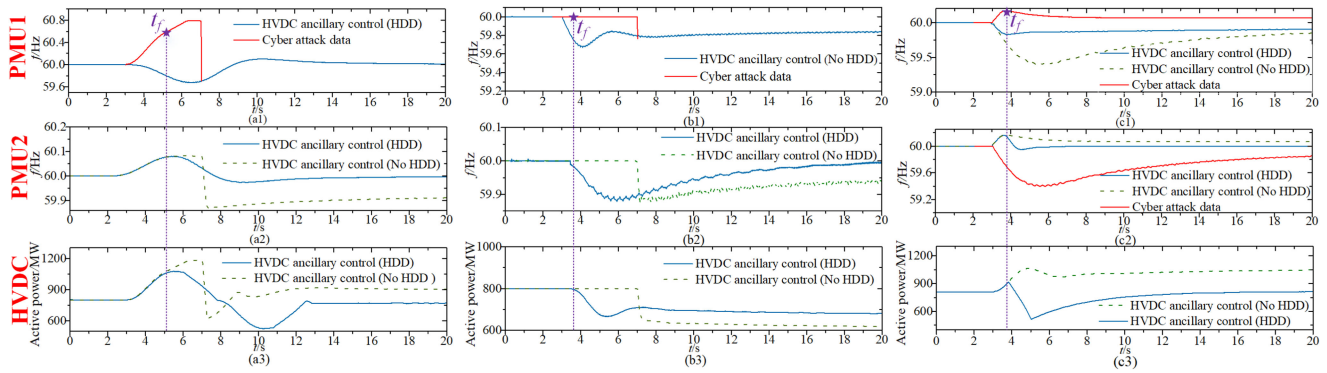


Fig. 7. Simulation result of the HDD-based HVDC ancillary control under different cyberattacks. (a1)–(a3) Ramping attack during [3 s, 7s],  $t_f = 5.1$  s. (b1)–(b3) Data loss attack during [3 s, 7s],  $t_f = 3.8$  s. (c1)–(c3) Data exchange attack during [3 s, 20s],  $t_f = 3.9$  s.

## VII. CONCLUSION

In this article, a hybrid data-driven based HVdc ancillary control strategy was proposed to detect and suppress the effects of FDIAs on the HVdc intertie operating stability. The attacked frequency type and duration time were quickly identified using the HDD. Different multikernels tests indicated that the MSVM can fully obtain the attack feature information using the real-world frequency data. The identification experiments with different attack intensity showed that the proposed HHT and MSVM could effectively identify five types of frequency attacks. The simulation verification of the HDD-based HVdc ancillary control was demonstrated based on a highly reduced power system model of the three North American interconnections. Based on the detected identification and duration time information in HDD, different comparison results revealed that the proposed HDD-based HVdc ancillary control could significantly suppress the impact of the frequency attacks on the HVdc intertie operation. In the future work, the MAC-based cyber defense method can be the promising directions for our research.

## REFERENCES

- [1] W. Wu *et al.*, "A virtual phase-lead impedance stability control strategy for the maritime VSC-HVdc system," *IEEE Trans. Ind. Informat.*, vol. 14, no. 12, pp. 5475–5486, Dec. 2018.
- [2] T. H. Nguyen, K. A. Hosani, and M. S. E. Moursi, "Alternating submodule configuration based MMCs with carrier-phase-shift modulation in HVdc systems for dc-fault ride-through capability," *IEEE Trans. Ind. Informat.*, vol. 15, no. 9, pp. 5214–5224, Sep. 2019.
- [3] L. Hong, Q. Xu, Z. He, F. Ma, A. Luo, and J. M. Guerrero, "Fault-tolerant oriented hierarchical control and configuration of modular multilevel converter for shipboard MVdc system," *IEEE Trans. Ind. Informat.*, vol. 15, no. 8, pp. 4525–4535, Aug. 2019.
- [4] K. Sun, H. Xiao, J. Pan, and Y. Liu, "A station-hybrid HVdc system structure and control strategies for cross-seam power transmission," *IEEE Trans. Power Syst.*, vol. 36, no. 1, pp. 379–388, Jan. 2021.
- [5] NREL, "Interconnections seam study," 2017. [Online]. Available: <https://www.nrel.gov/analysis/seams.html>
- [6] MISO, "MISO transmission expansion plan (MTEP)," MISO, 2014. [Online]. Available: <https://www.misoenergy.org/planning/>
- [7] J. Chand, "Auxiliary power controls on the nelson river HVdc scheme," *IEEE Trans. Power Syst.*, vol. 7, no. 1, pp. 398–402, Feb. 1992.
- [8] C. Lu, X. Wu, and E. A. J. Wu, "Implementations and experiences of wide-area HVdc damping control in china southern power grid," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2012, pp. 1–7.
- [9] B. J. Pierre *et al.*, "Design of the pacific dc intertie wide area damping controller," *IEEE Trans. Power Syst.*, vol. 34, no. 5, pp. 3594–3604, Sep. 2019.
- [10] F. Sass, T. Sennewald, and D. Westermann, "Automated corrective actions by VSC-HVdc-systems: A novel remedial action scheme," *IEEE Trans. Power Syst.*, vol. 35, no. 1, pp. 385–394, Jan. 2020.
- [11] R. Fan, J. Lian, K. Kalsi, and M. Elizondo, "Impact of cyber attacks on high voltage dc transmission damping control," *Energies*, vol. 11, 2018, Art. no. 1046.
- [12] A. Gholami, M. Mousavi, A. K. Srivastava, and A. Mehrizi-Sani, "Cyber-physical vulnerability and security analysis of power grid with hvdc line," in *Proc. North Amer. Power Symp.*, 2019, pp. 1–6.
- [13] K. Pan, E. Rakhshani, and P. Palensky, "False data injection attacks on hybrid AC/HVdc interconnected systems with virtual inertia-vulnerability, impact and detection," *IEEE Access*, vol. 8, pp. 141932–141945, 2020.
- [14] J. Dorn, H. Gambach, and J. Strauss, "HVdc and power electronic systems for overhead line and insulated cable applications B. 4-8 Trans Bay Cable - A breakthrough of VSC multilevel converters in HVdc transmission," in *Proc. CIGRE San Francisco Colloquium*, 2012, pp. 1–6.
- [15] 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.
- [16] S. P. Nandanoori *et al.*, "Model-agnostic algorithm for real-time attack identification in power grid using koopman modes," pp. 1–10, 2020.
- [17] 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.
- [18] Z. Yang, H. Liu, T. Bi, and Q. Yang, "Bad data detection algorithm for PMU based on spectral clustering," *J. Modern Power Syst. Clean Energy*, vol. 8, no. 3, pp. 473–483, 2020.
- [19] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, "Cyber risk analysis of combined data attacks against power system state estimation," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3044–3056, May 2019.
- [20] 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.
- [21] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems-attacks, impacts, and defense: A survey," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 411–423, Apr. 2017.
- [22] 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.
- [23] 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.
- [24] S. Sahoo, J. C. Peng, A. Devakumar, S. Mishra, and T. Dragiev, "On detection of false data in cooperative dc microgrids—A discordant element approach," *IEEE Trans. Ind. Electron.*, vol. 67, no. 8, pp. 6562–6571, Aug. 2020.
- [25] 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.

- [26] W. Qiu, Q. Tang, J. Liu, Z. Teng, and W. Yao, "Power quality disturbances recognition using modified s transform and parallel stack sparse auto-encoder," *Electric Power Syst. Res.*, vol. 174, 2019, Art. no. 105876.
- [27] S. Chen, X. Dong, Z. Peng, W. Zhang, and G. Meng, "Nonlinear chirp mode decomposition: A variational method," *IEEE Trans. Signal Process.*, vol. 65, no. 22, pp. 6024–6037, Nov. 2017.
- [28] M. Sahani and P. K. Dash, "Automatic power quality events recognition based on Hilbert Huang transform and weighted bidirectional extreme learning machine," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 3849–3858, Sep. 2018.
- [29] Y. Zhou, W. Chen, J. Gao, and Y. He, "Application of Hilbert-Huang transform based instantaneous frequency to seismic reflection data," *J. Appl. Geophys.*, vol. 82, pp. 68–74, 2012.
- [30] H. Liu and J. Xiang, "A strategy using variational mode decomposition, L-kurtosis and minimum entropy deconvolution to detect mechanical faults," *IEEE Access*, vol. 7, pp. 70 564–70 573, 2019.
- [31] J. Sun, Q. Xiao, J. Wen, and F. Wang, "Natural gas pipeline small leakage feature extraction and recognition based on LMD envelope spectrum entropy and SVM," *Measurement*, vol. 55, pp. 434–443, 2014.
- [32] P. G. V. Axelberg, I. Y. Gu, and M. H. J. Bollen, "Support vector machine for classification of voltage disturbances," *IEEE Trans. Power Del.*, vol. 22, no. 3, pp. 1297–1303, Jul. 2007.
- [33] K. R. Alik, "An efficient k-means clustering algorithm," *Pattern Recognit. Lett.*, vol. 29, no. 9, pp. 1385–1391, 2008.
- [34] J. Gilles, "Empirical wavelet transform," *IEEE Trans. Signal Process.*, vol. 61, no. 16, pp. 3999–4010, Aug. 2013.
- [35] A. Singh, B. S. Prakash, and K. Chandrasekaran, "A comparison of linear discriminant analysis and ridge classifier on twitter data," in *Proc. Int. Conf. Comput., Commun. Autom.*, 2016, pp. 133–138.
- [36] H. Shu, X. Zhao, H. Luo, and C. Li, "Research on stacking-based integrated algorithm of anomaly detection in production process," in *Proc. Int. Conf. High Perform. Big Data Intell. Syst.*, 2019, pp. 85–90.
- [37] 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, Jun. 2018.
- [38] 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.
- [39] T. Ma, Y. Jiang, H. Wen, B. Wu, X. Guo, and Z. Chen, "Physical layer assist mutual authentication scheme for smart meter system," in *Proc. IEEE Conf. Commun. Netw. Secur.*, 2014, pp. 494–495.
- [40] T. Matsumoto *et al.*, "Power system communications and information-theoretic cryptography," in *Proc. Transmiss. Distrib. Conf. Expo.: Asia Pacific*, 2009, pp. 1–4.
- [41] R. Sule, R. S. Katti, and R. G. Kavasseri, "A variable length fast message authentication code for secure communication in smart grids," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2012, pp. 1–6.
- [42] 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*, 2016, pp. 1–5.
- [43] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. S. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 675–685, Dec. 2011.
- [44] CURENT, "Current North American grid," 2018. [Online]. Available: <https://db.bettergrids.org/bettergrids/handle/1001/414>



**Wei Qiu** (Student Member, IEEE) received the B.Sc. degree in electrical engineering from Hubei University of Technology, Wuhan, China, in 2015, and the M.Sc. degree in instrumentation engineering in 2017 from Hunan University, Changsha, China, where he is currently working toward the Ph.D. degree in electrical engineering.

He is also a Joint Doctoral Student with the University of Tennessee, Knoxville, TN, USA, from 2019. His current research interests include power system analysis, cyber-security of synchrophasor, power quality measurement, and reliability analysis of power equipment.



**Kaiqi Sun** (Member, IEEE) received the B.S. and Ph.D. degrees in electrical engineering from Shandong University, Jinan, China, in 2015 and 2020, respectively.

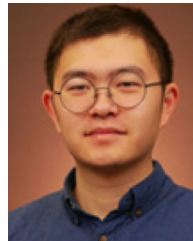
He is currently a Research Associate with the Department of Electrical Engineering and Computer Science, The University of Tennessee, Knoxville, TN, USA. He has authored or coauthored over 40 peer-reviewed technical articles or conference papers. His research interests include the control strategy of HVdc system and machine learning-based power system application.

Dr. Sun was the recipient of the Best Student Paper Award from IEEE IAS Industrial and Commercial Power System Asia Conference (IEEE IAS I&CPS Asia), the recipient of Excellent Paper Award from European Conference on Artificial Intelligence (ECAI), and the recipient of Best Paper Award from IEEE Student Conference on Electric Machines and Systems (SCEMS 2020).



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

He was a Research Associate with Oak Ridge National Laboratory, Oak Ridge, TN, from 2018 to 2020. He is currently a Professor with Hunan University. 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.



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

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

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

She is currently a Professor with Hunan University. Her current research interests include power system analysis, digital signal processing, and virtual instruments.



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

She is currently the Governors Chair with The University of Tennessee, Knoxville, TN, USA, and Oak Ridge National Laboratory (ORNL), Oak Ridge, TN, USA. She is elected as the Member of the National Academy of Engineering in 2016. 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, Blacksburg, VA, USA. 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.

