WAMS-Based HVDC Damping Control for Cyber Attack Defense

Kaiqi Sun, *Member, IEEE*, Wei Qiu, *Member, IEEE*, Yuqing Dong, *Student Member, IEEE*, Chengwen Zhang, *Student Member, IEEE*, He Yin, *Member, IEEE*, Wenxuan Yao, *Senior Member, IEEE*, and Yilu Liu, *Fellow, IEEE*

***Abstract*—Owing to the fast and large power regulating the capacity of the HVDC system, the wide-area measurement system (WAMS) based high voltage direct current (HVDC) system has been regarded as a prospective solution to deal with the low-frequency oscillation issue. However, due to the vulnerability of the WAMS communication, WAMS based HVDC system control can be a prime target of malicious penetrations that could lead to disastrous events. To remediate this adverse effect, an improved WAMS based HVDC damping control framework is proposed. First, a lightweight network named Attack Shuffle convolutional neural Networks (ASNet) is proposed to learn the characteristics of cyber attacks. Then, a model-free-based cyber attack defense framework is introduced to quickly identify the attack types based on the continuous wavelet transform and ASNet. Additionally, an improved control framework of the WAMS and HVDC-based wide-area power oscillation damping control (WH-PODC) is developed to provide different response control for mitigation of the impact of cyber attacks. Finally, the performance of the proposed WH-PODC control framework is evaluated with real PMU data in multiple scenarios in RTDS, where the results indicate that the response intensity can be kept under multiple types of cyber attacks while providing similar effectiveness in oscillation suppression to conventional controls.**

***Index Terms*—Wide-area measurement system, high voltage direct current system, cyber attack, low-frequency oscillation, damping control.**

I. Introduction

ELECTRIC power system is one of the largest and most complex man-made objects ever created [1]. Different from other forms of energy, electric energy has to be utilized or stored instantly as it is generated. Therefore, different types of controllers are configured to maintain the balance between demand and generation [2]. However, with the increasing penetration of renewable energies, the operational characteristics of the power system are changing [3]. Since most renewable energies are connected to the power grid via grid-connect converters (GCC) that do not provide inertia support to the power system, conventional controller designs based on the intrinsical generators may be inadequate for maintaining its operating stability with high renewable proportions [4]. Low inertia levels and power oscillations are becoming more frequent in daily power system operations [5].

Low-frequency oscillation (LFO) is a common problem that occurs when the generators lack damping torque [1]. Since GCCs under virtual synchronous generator (VSG) operation mode has similar dynamic performance as synchronous generators (SGs), the GCCs under VSG operation mode may interact with other GCCs or SGs in the low-frequency range and brings significant influence to the original LFO modes of the power system. [6], [7]. To suppress the LFO, a wide-area measurement system (WAMS) based power oscillation control has received much attention [8]. Due to its rapid and flexible power controllability, the high voltage direct current (HVDC) power system is one of the best carriers for realizing WAMS based oscillation controls. Various research has been conducted to investigate the LFO control via the HVDC systems, and some demonstration projects verified the performance of the WAMS and HVDC-based oscillation controls [9]–[11]. In [10], implementation of a wide-area damping controller is introduced to the Pacific dc Intertie (PDCI), which is an ±500 kV dc transmission line interconnecting the Oregon and California. In China, a wide-area adaptive damping control system coordinating multiple HVDC systems coordination was operated [11]. The experimental results of [11] indicate that the damping control can yield a 10% increase in the damping ratio of the dominant modes.

However, the remarkable performance of the HVDC system on LFO control is becoming a potential damage risk to the system oscillation control with the increasing cyber attack threats [12]. Recent research has demonstrated that the HVDC transmission damping control is vulnerable to cyber attacks, such as false data injection attack (FDIA) and replay attacks [13]. In the normal operation condition, benefiting from its fast power regulation ability, the HVDC system could provide

Manuscript received 9 September 2021; revised 21 December 2021; accepted 10 April 2022. Date of publication 19 April 2022; date of current version 22 December 2022. This work was supported by the National Natural Science Foundation of China under Grants U2166202 and 52177078. Paper no. TPWRS-01437-2021. *(Corresponding author: Wei Qiu.)*

Kaiqi Sun is with the School of Electrical Engineering, Shandong University, Jinan 250061, China (e-mail: skq@sdu.edu.cn).

Wei Qiu, Yuqing Dong, Chengwen Zhang, and He Yin are with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996 USA (e-mail: qwei4@utk.edu; yuqingdong0@gmail.com; czhang70@vols.utk.edu; hyin8@utk.edu).

Wenxuan Yao is with the College of Electrical and Information Engineering, Hunan University, Changsha 410082, China (e-mail: wenxuanyao@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 the 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/TPWRS.2022.3168078.

Digital Object Identifier 10.1109/TPWRS.2022.3168078

rapid response to significantly improve the dynamic damping ratio and thus mitigate the impact of LFOs [7]. However, if the measurements of Phasor Measurement Units (PMUs) are attacked, the control signal in response to the system LFO modes may be totally different from the system's actual needs. The fake control signal will make the HVDC system provides a wrong response to its connected AC system, which may be disastrous to the system operation [14]. Therefore, the configuration of the detection and mitigation methods against cyber attacks is essential before activating the HVDC and WAMS based LFO control.

Considering the significant impact of cyber attacks on the safe operation of power systems, research has been proposed to defend damping control systems. In [15], the information technology security system (ITSS) is proposed for deception attack detection. The simulation tests based on the 16-machine 68-bus AC/DC hybrid system reveal that the ITSS can successfully detect the attack when its level of spurious packets is higher than 30%. In [16], the dynamic loop WAMS based damping strategy is introduced and tested in the two-area and five-area IEEE benchmarks. However, this damping strategy is based on the assumption that the attack scenario is already known. To overcome this issue, the spoof catch and restore routine are presented to detect the synchrophasor spoofing by combining three spoof detectors [17]. And the linear state estimator is proposed to detect the FDIA for wide-area damping control [18]. However, this state estimation method requires system parameters, which limits the adaptability of cyber attack detection.

To remedy this, the data-driven methods provide a new perspective of cyber attack detection, which has the ability to learn patterns from measurement synchrophasors. For example, the random forest [19] and the back propagation neural network [20] are proposed for the detection of PMU data attacks. In addition, the Long-Short-Term-Memory (LSTM) is selected to differentiate cyber attack behaviors [21]. However, the detection time and the number of parameters are the main challenges of deep learning methods considering the response time requirements of WAMS based LFO controls. As discussed previously, the cyber attack, especially for the FDIA, has strong concealment and diversity, making it difficult and challenging to defend against in the WAMS based LFO controls.

This paper aims at mitigating the adverse effect caused by cyber attacks for the wide-area damping control. The contributions of this paper are as follows

1) To defend the HVDC damping control from cyber attacks, a lightweight network named Attack Shuffle convolutional neural Networks (ASNet) is proposed to learn the characteristics of multiple cyber attacks. The modified ShuffleNet V2 is introduced in ASNet to improve the detection accuracy.
2) Then, a model-free-based cyber attack defense framework is proposed to quickly distinguish the types of cyber attacks based on the Continuous Wavelet Transform (CWT) and ASNet. The advantage of the framework is that both the time and frequency domain features can be fused to highlight the attack information.
3) In order to involve the cyber attack detection function into the WAMS and HVDC-based wide-area power oscillation damping control (WH-PODC), an improved control framework of the WH-PODC is developed. In addition, a cyber attack defense control (CADC) is developed and integrated into the improved WH-PODC control framework to provide different response control for maximumly reducing the impact of cyber attacks.
4) Different experiments including cyber attack detection and three RTDS cases are conducted. The WH-PODC demonstrated solid performance in the testing, even under severe different cyber attacks.

II. Conventional WAMS and HVDC Based Low-Frequency Oscillation Control Framework

Due to potential poorly damped oscillation or even undamped oscillation that may limit the power transfer capability, LFO has become a necessary consideration for the secure and economic operation of power systems. Typically, the Power System Stabilizers (PSSs) configured at generators are adopted to mitigate LFO. However, the LFO modes in the power system are changing owing to the increasing integration of renewables and the retirement of conventional generators. Traditional PSSs usually use local information to generate the control signal. In addition, the parameters designation and tuning of the PSSs are often based on offline simulations so its parameters are usually not updated when in operation. Thus, in a power system with high renewable penetration, the oscillation control performance of the conventional PSSs may not perform as well as expected.

With the advancing of PMU-based synchronized measurement technology and power electronic technology, the WH-PODC has become a prospective solution for LFO suppression in power systems. Different from conventional LFO controllers, the WH-PODC is adaptive to accommodate various system operating situations, where its typical framework is shown in Fig. 1.

The working process of the WH-PODC contains five steps.

1) The PMUs configured in the AC grids measure the system voltage phasors and then calculate the frequency based on the measured data.
2) After calculating and data packaging, the frequencies in different AC grids are delivered from PMUs to Phasor Data Concentrators (PDCs). The specific communication protocol, such as IEEE C37.118 [22], is adopted in the communication process for security and accuracy requirements.
3) When the PDCs receive the frequency data, they unpackage and send the frequency data to WH-PODC.
4) The block diagram of the WH-PODC is shown in Fig. 2. The objective of the WH-PODC is to improve the system damping ratio to enhance the system stability during oscillation. As shown in Fig. 2, the WH-PODC calculates the frequency difference Δf_{PMU} based on the frequency data from two different PMUs. Then the Δf_{PMU} is converted to active power control order P_{PODC} via the control block in Fig. 2.
5) The converted P_{PODC} is added on constant active power control in the outer loop of the HVDC system to modify the power flow to actuate the oscillation damping control.

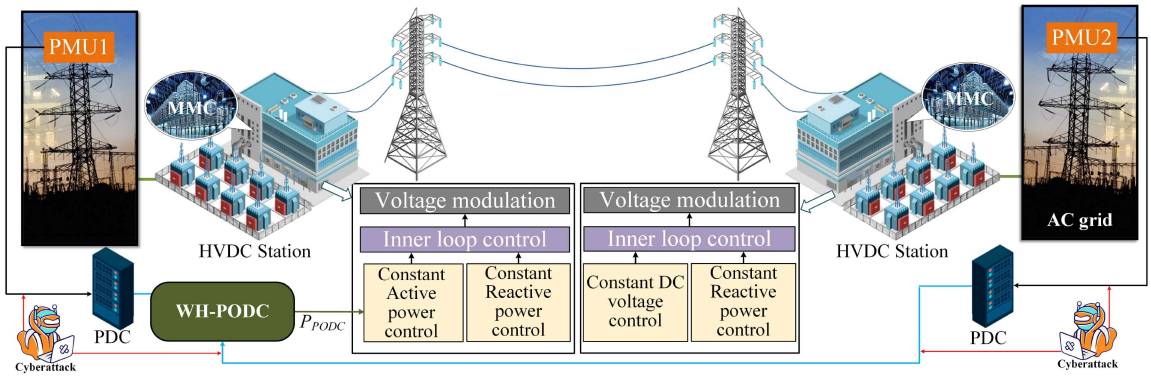


Fig. 1. The typical framework of the HVDC system with WH-PODC.

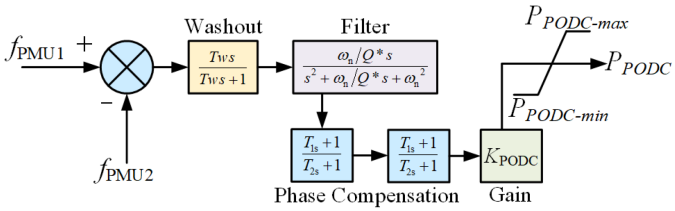


Fig. 2. The block diagram of the WH-PODC, where the f_{PMU1} and f_{PMU2} are the frequency data from two different PMUs, the T_w is the time constant that is usually set as 10 s, the s is Laplace factor, ω_n is the oscillation frequency of the targeted mode, which is related to the system operating configuration. Q is the quality factor that is usually set as 1, the T_1 and T_2 are the time constant, the K_{PODC} is the droop coefficient, the P_{PODC} is the power output of the WH-PODC, and the $P_{PODC-max}$ and $P_{PODC-min}$ are the maximum and minimum limit of the P_{PODC}.

Due to the low cost and high efficiency, cyber attack meets continuously increase in different types of cyber physical systems. In May 2021, the largest gas pipelines in the U.S. were forced to shut down because of the cyber attacks, which exposed the vulnerability of conventional communication infrastructure [23]. As reported by the French think-tank Institut Français des relations internationals (IFRI), the power system is becoming a primary cyber attack target in recent years [24]. Moreover, in 2016, one substation in Ukraine became a target of cyberattacks, which led to an outage in part of Kyiv for an hour [25].

Because the HVDC system possesses fast power regulating capacity and needs communication in the control process, the WH-PODC has the possibility to be a prime target that is maliciously penetrated by attackers. As shown in Fig. 1, the cyber attack could be applied in the communication between the PMUs and PDCs, or applied in the communication between the PDCs and WH-PODC. Both ways of cyber attacks will result in an erroneous response of the WH-PODC, which may significantly affect the system operating safety. Hence, it is critical to investigate potential solutions to rapidly and accurately detect cyber attacks targeting WH-PODCs.

III. Model-Free-Based Cyber Attack Defense

To improve the control performance under cyber attacks, the first step of WH-PODC is to detect the types of attacks so that their impact can be mitigated.

A. Data Preprocessing

The motivation of data preprocessing is to remove the redundant components and highlight the characteristics of the attack signal in the measurement data. Here, the redundant components refer to the trend data or DC component. Some studies in [26], [27] have shown that the trend component is redundant information that can be removed from the measurement data.

Denoting the i_{th} PMU measurement data as $x_{di}(t)$, to remove the trend component, a high pass filter is used before the feature extraction process. Thereafter, the output of detrended data becomes $x_i(t)$.

To fully simulate the impact of different attacks, four types of cyber attacks are selected, including the false oscillation attack (L_1), replacement attack (L_2), noise attack (L_3), and data loss attack (L_4) [28]. These four attacks will directly affect the frequency and damping ratio parameter estimation of low frequency oscillations.

B. Time-Frequency Feature Extraction of Attacked Data

To identify the attacked measurement data, the CWT is utilized to extract its unique fingerprint. The advantage of CWT is that both time-domain and frequency-domain features can be reflected. Compared with the commonly used single time domain or frequency domain analysis algorithm, such as the Empirical Mode Decomposition (EMD) and FFT, the CWT has the potential to provide richer two-dimensional joint information for the attacked signal [29].

The CWT of $x_i(t)$ can be calculated as

$$w_x(\tau, s) = \frac{1}{\sqrt{s}} \int_{-\infty}^{+\infty} x_i(t) \psi^* \left(\frac{t-\tau}{s} \right) dt \qquad (1)$$

where the $\psi^*(\frac{t-\tau}{s})$ is the mother wavelet which can be used to create a set of wavelets functions, $*$ is the complex conjugate, the τ, and s are the position and scale parameters, respectively.The results w_x of the is a complex matrix and the modulus $|w_x|$ of w_x can be calculated so that the classifier can be detected.

The decomposition performance of the CWT is determined by the mother wavelets functions. To this end, a suitable wavelet can be selected from a set of alternative wavelets, such as the Morlet, Gaussian, Mexican hat, and Haar wavelet functions [30].

Specifically, the time and frequency resolutions are two critical indicators to determine the decomposition performance.

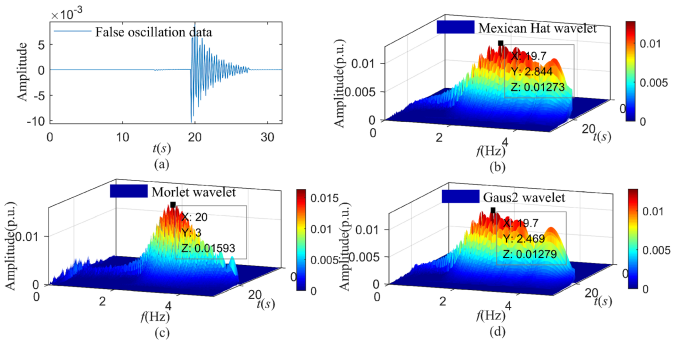


Fig. 3. The false oscillation data and its CWT results with different wavelet functions. (a) the false oscillation data, (b) Mexican Hat wavelet, the energy is 21.6278, (c) Morlet wavelet, the energy is 19.9526, (d) Gaus2 wavelet, the energy is 21.4522.

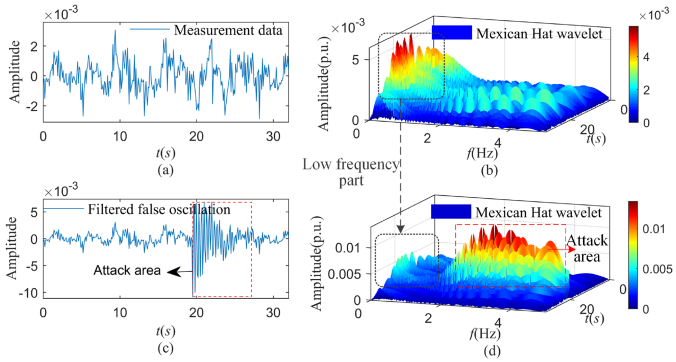


Fig. 4. The measurement data and the attacked false oscillation data. (a) measurement data, (b) the CWT of (a), (c) the filtered false oscillation data, (d) the CWT of (c).

Here, the resolution indicates the ability to distinguish different component signals, so the higher resolution results, the better. For example, the results usually have a better time resolution if the boundary between the two components is clearer. Meanwhile, the more concentrated energy usually comes with a higher resolution, since energy is another statistical feature to help filter the results, which can be expressed as

$$E_w = |w_x(\tau, s)|^2 \tag{2}$$

C. Attack Detection Using CWT

To select the suitable wavelets function, three wavelets are selected from a set of wavelets functions, including the Morlet, Gaussian, and Mexican hat [30]. It is mainly the characteristics of the attack signal rather than the measurement data to determine whether the data are attacked or not. An example of false oscillation data is analyzed, as shown in Fig. 3.

In this test, an oscillation with a 0.01 p.u. magnitude is simulated in Fig. 3(a). It shows that all the CWTs can detect the time-frequency features of the oscillation. The spectrum leakage, defined as the false spectra with smaller amplitudes caused by the non-coherent sampling [31], can work with energy as the criterion to select a suitable wavelet.

Fig. 3(c) shows that it contains a frequency component near 0 Hz caused by the spectrum leakage. As for 3(b) and (d), it can be seen that the results of CWT are similar, and it is difficult to evaluate the results from the perspective of spectrum leakage. However, the energy of the Mexican Hat wavelet is 21.6278, which is higher than the Gaus2 wavelet. This means its energy is more concentrated under the similar condition of spectrum leakage. Therefore, the Mexican hat is selected as the wavelets based on its decomposition effect.

To verify the decomposition result of the attacked signal, the CWTs of measurement data and false oscillation attacked data are presented in Fig. 4. Here, the false oscillation attack is selected as an example. Fig. 4(a) is the measurement data (normal value), and Fig. 4(b) is its CWT results. As can be seen in Fig. 4(b), the main frequency components are located in low frequency part (<2 Hz). The amplitude is about 5×10^{-3}. For the false oscillation attacked data in Fig. 4(c), a higher frequency component (red rectangle in Fig. 4(d)) appears near the 20 s–28 s.

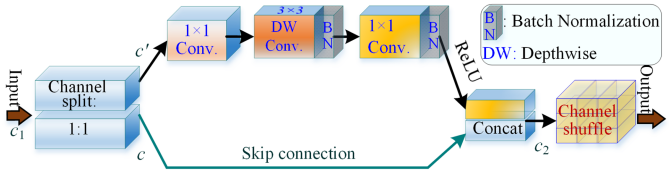


Fig. 5. The structure of ShuffleNet V2.

The amplitude of the attacked signal is higher than the lower frequency part. Thus, the normal frequency components are weakened. Based on this difference, the attacked data can be detected. Compared with Fig. 4(b) and (d), the frequency of the measurement data is covered up because the false oscillation has a higher amplitude. This test shows that the CWT has the ability to detect the characteristics of the attack signal due to the differences in the time-frequency information.

D. Attack Identification Using ASNet

After obtaining the CWT $w_x(\tau, s)$ of the attacked signal, a classifier is required to identify the type of cyber attacks so that the WH-PODC system can be optimized. The traditional model-free-based machine learning methods have the ability to classify different features. However, there is numerous data that collected continuously which may limit the performance of the traditional machine learning methods. To this end, an ASNet is proposed to provide real-time decisions to the LFO damping control.

The ASNet is built upon the basic convolutional neural networks (CNN) architecture, where CNN consists of the convolutional layer, pooling layer, and fully connected layer [32]. The detection performance can be improved by learning the relationships from the input and output data of CNN. The response time of the damping control requires the classifier to finish classification in a limited time. However, the CNN suffers from a large number of parameters in order to achieve sufficient performance, which increases the time cost. To mitigate this problem, the lightweight shuffle CNN (SCNN) is proposed, where the ShuffleNet V2 is integrated into the CNN.

The structure of ShuffleNet V2 is shown in Fig. 5. The advantage of ShuffleNet V2 is that it can reach a better state in terms of speed and accuracy [33]. The ShuffleNet V2 utilizes two

strategies to make the structure compact, including the channel split and channel shuffle.

As shown in Fig. 5, the input features will be split into two branches first in the channel split procedure, where these two branches have an equal number of channels c and c' to minimize Memory Access Cost (MAC). The MAC reflects the calculation speed in the hardware implementation, e.g., GPUs, which can be defined as below

$$MAC = hw(c_1 + c_2) + c_1 c_2 \tag{3}$$

where the h and w denote the height, width of the feature map, respectively. And c_1, and c_2 are the number of input channels and output channels, respectively. The $hw(c_1 + c_2)$ denotes the memory access for input/output feature maps, and $c_1 c_2$ are the kernel weights. Theoretically, a model with less feature map and a lower number of channels will have a lower MAC and a higher calculation speed. The c_1 and c_2 are set as the same because ShuffleNet V2 would have the lowest MAC when $c_1 = c_2$ [33].

In the upper branch of Fig. 5, the c' channel will conduct the 1×1 convolutions and depthwise convolution (DW Conv.). The DW convolution is a type of element-wise operator that has a lower MAC [34]. The second channel c is directly connected to the output of the c' channel, which is called skip connection. The process is a kind of feature reuse with the ability to reduce redundancy and accelerate calculation. Then the output of ShuffleNet V2 becomes c_2 by channel concatenate operation. Thereafter, the channel shuffle is connected, where it will rearrange the features according to a certain rule to cross information flow for these two branches [35]. It can promote feature fusion by changing the direction of features.

However, the last layer of the ShuffleNet V2 uses the global average pooling, where the maximum value is retained and some key information will be lost. To overcome this issue, the attack shuffle CNN is proposed where the Depthwise Separable (DS) convolutional layer and the (parametric rectified linear unit, PReLU) are used to replace the global average pooling in ASNet. The output of the DS convolution will increase the diversity of features and the output of ASNet will be more flexible. Meanwhile, the PReLU can improve the fitting ability and reduce the risk of overfitting for the model [36], of which the output can be expressed as

$$PReLU\,(d_s) = \begin{cases} d_s, & \text{if } d_s > 0 \\ a_i d_s, & \text{if } d_s \le 0 \end{cases} \tag{4}$$

where the d_s is the output of the DS convolution, the a_i is the learnable negative slope. The PReLU can avoid convergence difficulties when a larger learning rate is set in ASNet.

The structure of the proposed ASNet is shown in Fig. 6. The shuffle block refers to the ShuffleNet V2 and it can be stacked. Then the DS convolutional layer is connected to the shuffle block. Finally, the fully connected layer with the softmax function is used to classify the CWT $w_x(\tau, s)$.

E. Attack Defense CWT-ASNet Framework

Integrating the CWT and ASNet, a cyber attack identification framework called CWT-ASNet is proposed to improve the damping control. As shown in Fig. 6, the CWT-ASNet framework consists of two steps

1) Calculating the CWT: The PMU data $x_{di}(t)$ is filtered to remove the DC component and get $x_i(t)$. Then CWT of $x_i(t)$ is calculated to obtain the time-frequency features w_x of the attacked data signal. The $x_i(t)$ is down-sampled to (160, 80) to speed up the calculation.
2) Identifying the cyber attack: The ASNet is constructed to identify the cyber attacks, where the output label of the ASNet is L_i. The L_0 is the normal measurement data, and the L_i, $i = 1, 2, 3, 4$ denotes four types of cyber attacks. The L_i will be sent to the damping control step in WH-PODC.

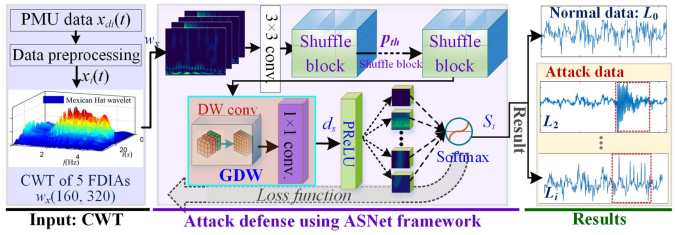


Fig. 6. Framework of the proposed improved CWT-ASNet.

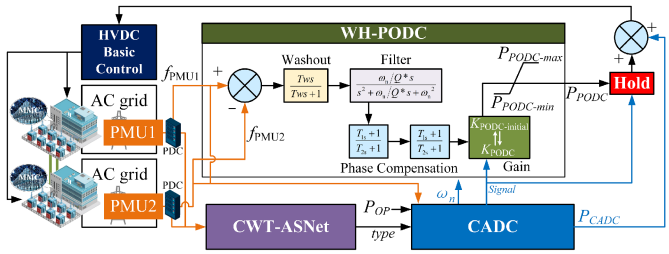


Fig. 7. The control framework of improved WH-PODC with CWT-ASNet, where CADC is the cyber attack defense control, the P_{CADC} is the power output of the CADC, the P_{OP} is the operating power flow on the HVDC system and the $K_{PODC-initial}$ is the initial droop coefficient of the WH-PODC before getting the detecting result.

IV. Novel WAMS and HVDC Based Low-Frequency Oscillation Control With CWT-ASNet

The proposed CWT-ASNet is expected to detect the cyber attacks in a short time, which includes the presence of cyber attacks and types of attacks if any. The WH-PODC with the proposed attack defense CWT-ASNet framework could significantly improve the operating safety of the HVDC system with the WH-PODC when it is under potential cyber attacks. Next, the improved WH-PODC framework will be introduced in the following subsections in detail.

A. Improved WAMS and HVDC Based Low-Frequency Oscillation Control Framework

The detailed control framework of improved WH-PODC with CWT-ASNet is shown in Fig. 7.

As shown in Fig. 7, the attack defense CWT-ASNet framework is integrated into the WH-PODC in order to provide fast

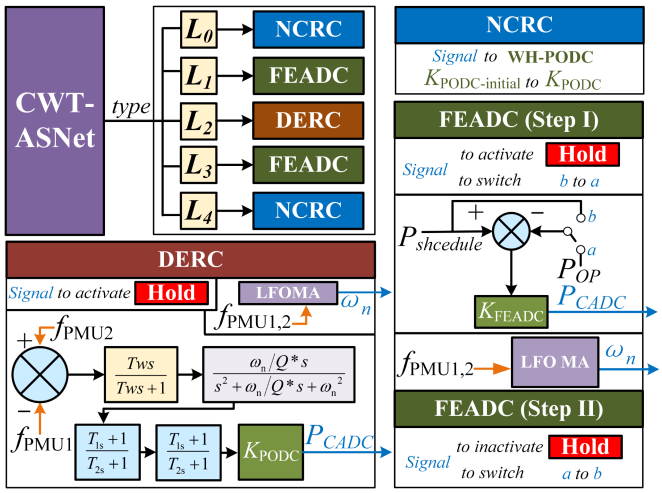


Fig. 8. The control framework of improved WH-PODC with CWT-ASNet, where CADC is the cyber attack defense control, LFOMA is LFO model analysis, and the $K_{PODC-initial}$ is the initial droop coefficient of the WH-PODC before getting the detecting result, the K_{PODC} is the droop coefficient used in the NCRC of WH-PODC. The $K_{PODC-initial}$ and K_{PODC} are determined according to the grid code.

and accurate cyber attack detection. The improved WH-PODC control framework could be described as follows:

1) The PDCs send f_{PMU1} and f_{PMU2} to not only conventional WH-PODC, but the attack defense CWT-ASNet framework as well for cyber attack detection.
2) During the detection process of the CWT-ASNet, the conventional WH-PODC will keep working with a smaller droop coefficient $K_{PODC-initial}$. The aim of $K_{PODC-initial}$ is to keep part of the response capability of the WH-PODC, so that it still provides a certain response to the system LFO while reducing the effect caused by the potential cyber attacks.
3) After the CWT-ASNet concludes, the detection results, including the presence and types of potential cyber attacks, are delivered to the CADC for finalizing appropriate response strategies to mitigate the cyber attacks' impact on the WH- PODC.

The detailed control strategies of the CADC are described below.

B. Improved WH-PODC Control Framework for Cyber Attack Defense

In order to balance the fast response requirement and cyber attack defense need, in this paper, a cyber attack defense control (CADC) is proposed for the improved WH-PODC control framework. The CADC is based on the detection results of the CWT-ASNet. According to the different types of cyber attacks, the CADC will provide different response control in order to maximumly reduce the impact caused by the cyber attack.

Based on the cyber attack classification in Section III-A, the detailed control strategies of the proposed CADC are depicted in Fig. 8.

As shown in Fig. 8, when the CWT-ASNet finishes the detection, the CWT-ASNet will send the detecting results L_i to CADC for returning to the normal responses or switching response strategies according to the type of the cyber attacks. According to the type of cyber attacks, three control strategies are defined in the CADC:

1) Normal Operation Condition Recovery Control (NCRC)
2) Fake Event Attack Defense Control (FEADC)
3) Data Exchange Recovery Control (DERC)

$NCRC$: When the detecting result of the CWT-ASNet is L_0 or L_4, the NCRC is adopted in the CADC. The objective of NCRC is to recover the WH-PODC full response capability in order to provide enough power support to mitigate the LFO. When the NCRC is activated, the NCRC sends a signal to WH-PODC to change the Gain from $K_{PODC-initial}$ to K_{PODC} to provide the normal response capability of the WH-PODC.

$FEADC$: When the detecting result of the CWT-ASNet is L_1 or L_3, the FEADC is adopted in the CADC. The FEADC is designed to realize a fast WH-PODC recovery from the fake event attack. The control process of the FEADC could be described as:

1) When the FEADC is activated, the FEADC sends a signal to the "Hold" function to freeze the output of the WH-PODC. Meanwhile, the FEADC also sends a signal to the switch module to change the switch from node "b" to node "a". With the switch change, the output (P_{CADC}) of the FEADC (Step I) is modified from equation (5) to equation (6), which could help recover the wrong response of the WH-PODC. In addition, the wrong response may cause the system dispatch change. In order to guarantee that the "ω_n" is still appropriate during the recovery process, the LFO model is reanalyzed.

$$P_{CADC} = 0 \tag{5}$$

$$P_{CADC} = P_{schedule-POP} \tag{6}$$

2) When the signal from CWT-ASNet is changed to "L_0," the FEADC will send the signal to inactivate the "Hold" function to release the output of the WH-PODC while changing the switch from node "a" to node "b" to stop FEADC.

$DERC$: When the detecting result of the CWT-ASNet is L_2, the DERC is adopted in the CADC. The DERC aims at mitigating the influence of the replacement attack and providing fast support to recover the normal WH-PODC response. The control process of the DERC could be described as:

1) When the DERC is activated, the DERC sends a signal to the "Hold" function to freeze the output of the WH-PODC. Meantime, the wrong response may cause the system dispatch to change. In order to guarantee an appropriate "ω_n," the LFO model is reanalyzed during the recovery process.
2) When a correction of the "ω_n" is determined and is sent to WH-PODC, the recovery function in the DERC is activated to provide correct WH-PODC response to the system in order to suppress the influence of the replacement attack.

V. Experiments and Analysis

To verify the performance of the proposed CWT-ASNet and the improved WH-PODC control framework, multiple

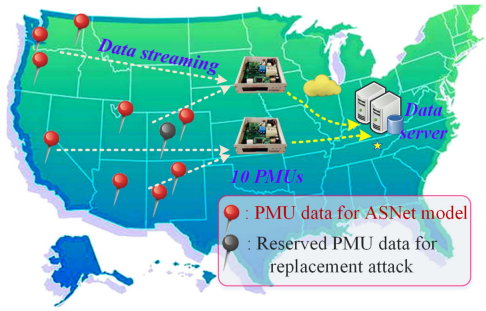


Fig. 9. PMU data source from ten locations.

TABLE I
PERFORMANCE COMPARISON UNDER DIFFERENT CLASSIFICATION METHODS

Models	Num. of Conv./shuffle (%)			Num. of parameters	Test time (ms)
	2	4	8		
LSTM	91.59	93.61	94.65	457k	1.62
FFT-1DCNN	89.24	88.62	88.64	72k	0.43
CWT-2DCNN	94.69	95.19	94.87	171k	0.61
CWT-SCNN	97.43	97.46	97.72	28k	0.50
CWT-ASNet	**97.45**	**97.60**	**97.77**	17k	0.47

experiments are carried out in python and Real-Time Digital Simulator (RTDS) separately. The actual PMU data from the WECC system are used to generate the simulated data set and it is related to the physical network. 10 PMUs are selected, and one of the PMU is reserved for replacement attack, as shown in Fig. 9. Particularly, 39240 samples are generated, of which 70% are used as the training set, 15% for verification, and the rest for testing. Meanwhile, the data from three different time instants are selected to verify the time sensitivity of the CWT-ASNet, including the 01-05 (January 5th), 01-25 and 04-05 in 2019. Totally 5580 samples are collected for each time instant, where the length of each sample is 320 with a 10 Hz reporting rate. Besides, three PMUs data with a 120 Hz reporting rate are also used to verify the real-time performance of CWT-ASNet.

A. Comparison of Different Attack Identification Methods

To verify the effectiveness of the proposed ASNet method, different classifiers are selected, including the Two-dimensional Convolutional Neural Network (2DCNN), LSTM, One-dimensional Convolutional Neural Network (1DCNN), and SCNN. The detection performance is listed in Table I.

For the 1DCNN, 2DCNN, and LSTM, 2, 4, and 8 conventional layers are selected to verify their performance. For SCNN and ASNet, the numbers 2, 4, and 8 mean 2, 4, and 8 shuffle blocks. Meanwhile, the number of parameters of the classifier and the testing time of each sample is provided. It should be noted that only the time cost of the classifier is calculated for a fair comparison in this test.

It can be seen that the performance of LSTM is higher than FFT-1DCNN because the information of FFT is insufficient for classification. However, the LSTM consumes 1.2 ms more time than the 1DCNN. Compared with FFT-1DCNN, the accuracy of CWT-2DCNN is 5% higher. The main reason is that both the time and frequency domain information are extracted in CWT,

TABLE II
PERFORMANCE COMPARISON WITH STATE-OF-THE-ART METHODS

Models	Feature extraction	Accuracy (%)			Test time (ms)
		01-05	01-25	04-05	
FFT-BP [27]	automatic	82.52	78.04	71.52	5.95
MM-RFC [19]	manually	79.51	75.40	70.29	1.81
MM-gcForest [26]	manually	88.63	82.85	76.13	1.96
EEMD-FFT-BP [20]	automatic	81.39	67.02	54.46	82.29
CWT-ASNet	automatic	**97.60**	**96.99**	**95.53**	28.76

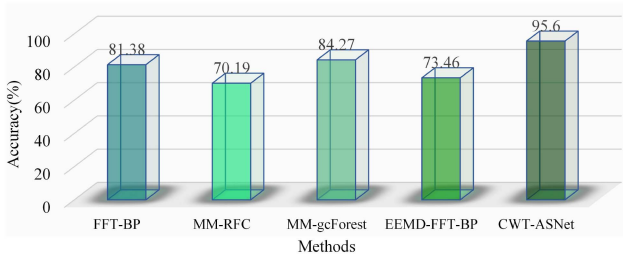


Fig. 10. Performance comparison with 120 Hz reporting rate.

which provides an expanded feature space. The CWT-SCNN obtains 3% higher performance than CWT-2DCNN even with fewer parameters. Moreover, the proposed CWT-ASNet obtains the highest accuracy of 97.77% and the minimum number of model parameters (17 k). This is due to the ShuffleNet V2 and DS conventional layer's contribution to parameter compression and feature diversity. Overall, a CWT-ASNet with 4 shuffle clocks is selected as the final structure with a balance between accuracy and the number of parameters.

B. Comparison With State-of-The-Art Methods

To verify the proposed framework with the state-of-the-art approaches, four cyber attack detection methods are compared including the FFT-BP [27], MM-RFC [19], MM-gcForest [26], and EEMD-FFT-BP [20]. Importantly, the data from three time instants are used to verify the robustness of different approaches, where the results are listed in Table II.

The results show that the performance of MM-RFC is only 79.51% on the 5th of January. However, it consumes less time because only the statistical features are fed into RFC, which has a smaller size. With the increase of time instants, the accuracy decreases for all the methods since the load condition in the power system is different. For EEMD-FFT-BP, the accuracy becomes only 54.46% on the 5th of April, indicating the distinguishable features are lost for the cyber attack signal. It also consumes 82.29 ms because the EEMD needs to perform multiple decompositions. The accuracy between the 5th of January and the 5th of April is various. For example, the accuracy differences of FFT-BP and MM-gcForest are 11% and 12.5%, respectively. However, 2.03% accuracy difference is obtained for CWT-ASNet, indicating that it has better robustness. The test time of CWT-ASNet is 28.76 ms, which can meet the requirements of real-time damping control.

To verify the performance with 120 Hz data reporting rate, one-day data are used from three PMUs located in the same city. The detection results are shown in Fig. 10. It can be seen

TABLE III
PERFORMANCE UNDER THE DIFFERENT NUMBER OF TRAINING SAMPLES

Model	Acc. with different ratios of samples(%)				
	5%	10%	20%	50%	70%
CWT-ASNet	87.55	91.20	93.047	94.56	95.53

that the MM-gcForest gets an 84.27% accuracy, 10% higher than EEMD-FFT-BP. Compared with the result in Table II, the accuracy of the proposed method is 2% lower. This is because the data are similar due to the fact that they are collected from the same city, which makes it challenging for detection and identification. Overall, the proposed method obtains better performance at various even at different data reporting rates.

Besides, to provide the theoretical guarantees, the statistical learning theory and the shattering coefficient can be used. According to [37], the number of neurons per layer and along layers is what mostly influences the algorithm bias. And by having enough training examples, the learning convergence can be proved. On the other hand, learning cannot be ensured if the training examples are not sufficient, and results may be changing [37]. Meanwhile, according to [38], a change of the labeled data for each source can also be resulting in a tighter bound. This means that the performance of the models depends on the number of training examples as well as the structure of the model.

To verify the performance of CWT-ASNet under different ratios of training samples, 10%, 20%, 50%, and 70% of samples are used to train the model. The results are listed in Table III.

As can be seen in Table III, it shows that the performance will decrease if the ratio of the training samplings decreases. The lowest accuracy is 87.55% when the ratio is 5%. And the performance is higher than 94.5% when the ratio is higher than 50%. The conclusion can be drawn that: for a specific method, the bound of the prediction accuracy (or the lowest performance) can be determined by its structure and ratio of training samples.

To select an appropriate method in practical applications, more factors and comparisons need to be considered. Meanwhile, the comparison is meaningful if the external parameters (such as the input data, operating environment, and training samples) are the same. Therefore, the prediction error of one method may stay above or below of another if the external parameters are the same except for the method. As shown in Table II in Section V-B, the CWT-ASNet always performs better with a high probability (more than 50%) with the same external parameters. There are still some exceptions. For example, the EEMD-FFT-BP outperforms the MM-RFC in 01-05-2019, as shown in Table II. However, the accuracy decreases rapidly to 54.46%, and EEMD-FFT-BP obtains lower accuracy than MM-RFC in 04-05-2019. The probability is 50% when comparing the EEMD-FFT-BP and MM-RFC. This is to say that one method can perform better in one tested time. It does not mean that it will always perform better than the other.

As the saying goes, every coin has two sides. A model with higher accuracy may also be more complex. For example, the proposed method consumes more time than MM-RFC [19] and MM-gcForest [26]. The user needs to select the appropriate approach according to actual needs because one method is almost impossible to fulfill all requirements.

Overall, the proposed method obtains a higher probability that it outperforms than the other four methods. This probability can vary when comparing with different methods.

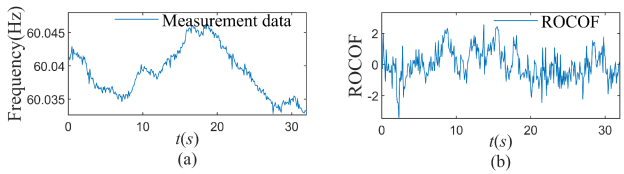


Fig. 11. ROCOF of the measurement data.

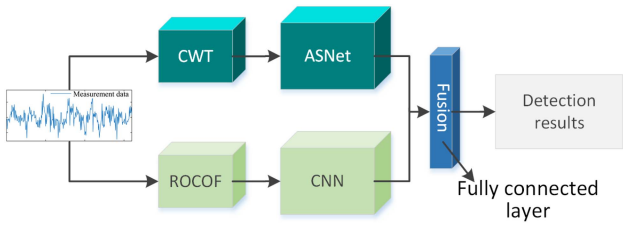


Fig. 12. Fusion structure of the CWT-ASNet and physical-based feature.

TABLE IV
COMPARISON OF PHYSICAL-BASED MODEL

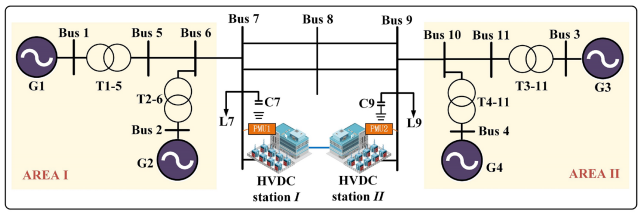
Models	Accuracy (%)		Test time (ms)
	01-05	04-05	
CWT-ASNet	97.60	95.53	28.76
ROCOF-CNN	96.00	87.76	0.45
Fusion model	97.55	95.42	29.19

C. Exploration of Physical Information

Physical information reflects the operating status of the power system. To explore the contribution of physical information to cyber attack detection. The rate of change of frequency (ROCOF), as a key indicator of network stability and the balance between electricity supply and demand, is selected as the objective physical information. It can be inferred from the frequency measurement. In this test, the duration is set to 0.5 s (10 Hz reporting ratio), and the ROCOF of the measurement data is shown in Fig. 11.

To incorporate the ROCOF into the proposed CWT-ASNet, a fusion network with two inputs is designed, which contains two branches. Then their outputs will be added to form one vector so that the final decision can be made. The structure of this fusion network is shown in Fig. 12. As can be seen from Fig. 12, the ROCOF is learned in a three-layer CNN and the output of these two branches is connected in the fully connected layer.

The detection results of these three models (CWT-ASNet, ROCOF-CNN, and fusion models) are listed in Table IV. It can be seen that the performance of the CWT-ASNet is similar to the Fusion model. However, the accuracy of ROCOF-CNN in 04-05 (means April 5th in 2019) is much lower than the CWT-ASNet and Fusion models because the information from CWT is richer than ROCOF. The cost time of the fusion model is slightly



(a)

(b)

Fig. 13. The diagram of the modified two-area Kunder system and the RTDS test system. (a) The topology of the modified two-area Kunder system. (b) The RTDS experimental environment.

TABLE V
MAIN CIRCUIT PARAMETERS OF THE HVDC SYSTEM

Parameters	Value
Rated powerof MMC/MVA	800
Nominal voltage of MMC/kV	±320
Rated DC current of MMC/kA	1.25
Rated power of Converter transformer/MVA	840
Nominal voltage of converter transformer/kV	230/304
Leakage impedance of converter transformer/%	16
Inductance of star point reactor/H	5000
Resistance of star point reactor/k Ω	5
Number of sub-module per valve arm	350
Individual capacitance/mF	20.57

higher than CWT-ASNet. Overall, the ROCOF contributed to the identification of attacks, and the customer can merge the ROCOF into their own model since it reflects some physical characteristics of the grid.

D. Verification of Improved WH-PODC Control Framework

Next, to verify the effectiveness of the improved WH-PODC control framework with CWT-ASNet, in this subsection, three case studies are conducted in the modified two-area Kunder system in RTDS. The test system is modified from a two-area Kunder system [39]. The diagram of the modified two-area Kunder system and the RTDS test system is shown in Fig. 13.

As shown in Fig. 13, the modified two-area Kunder system is comprised of 11 buses, 4 synchronous generators, and 2 areas. Different from the original two-area Kunder system, the two areas are connected through one HVDC system in addition to the two AC tie lines. The main circuit parameters of the HVDC system configured in the test system are listed in Table V. The control parameters of the WH-PODC are listed in Table VI.

As shown in Fig. 13, the modified two-area Kunder system is comprised of 11 buses, 4 synchronous generators, and 2 areas.

TABLE VI
CONTROL PARAMETERS OF THE WH-PODC

Parameters	T_w	Q	W_n	T_1/T_2	K_{PODC}	$\frac{P_{PODC-max}}{P_{PODC-min}}$
Values	10	1	4.27	1	40	±80

Different from the original two-area Kunder system, the two areas are connected through one HVDC system in addition to the two AC tie lines. The objective of using RTDS to verify the proposed CWT-ASNet and the improved WH-PODC control framework is to provide a real-time hardware in the loop (HIL) environment ready, so that the testing of the control devices can be implemented on hardware in the near future. The main circuit parameters of the HVDC system configured in the test system are listed in Table V. The control parameters of the WH-PODC are listed in Table VI.

In this section, the normal operating condition and two different types of cyber attacks, false oscillation attack (L_1) and replacement attack (L_2), are used to verify the performance of the improved WH-PODC control framework. The cyber attacks are simulated according to real oscillation event data.

1) Case I: Normal Operating Condition Test Scenario: Under the initial condition, the power flow on the HVDC system is 400 MW. An oscillation occurred at $t = 3$ s in the system. The Fig. 14(a1), Fig. 14(b1), and Fig. 14(c1) show a performance comparison of the improved WH-PODC control framework and traditional WH-PODC under no cyber attack condition.

As shown in the Figures, at the beginning of the oscillation event, different from the traditional WH-PODC, the improved WH-PODC control framework is activated first in order to detect the presence of potential cyber attacks. During the detection process, the HVDC response in the improved WH-PODC control framework is smaller than the traditional WH-PODC, as shown in Fig. 14(c1). Around $t = 3.3$ s, the detection results are obtained from the CWT-ASNet and sent to CADC. The CADC adopts NCRC to provide the necessary support to Area I according to the CWT-ASNet signal. As demonstrated by the simulation results, the CWT-ASNet detection process may take some time, which causes the supportability reduction of the WH-PODC. However, as shown in Fig. 14(a1) and Fig. 14(b1), the frequency oscillation is suppressed in a similar time. The simulation results indicate that the control performance of the WH-PODC is only slightly influenced. The response of the WH-PODC in the improved control framework is still timely and effective for the LFO mitigation.

2) Case II: False Oscillation Attack Test Scenario: Under the initial condition, the power flow on the HVDC system is 400 MW. At $t = 3$ s, the PMU1 starts to experience a false oscillation attack that lasts until $t = 5$ s. The Fig. 14(a2), Fig. 14(b2) and Fig. 14(c2) shows the performance comparison of the improved WH-PODC control framework and traditional WH-PODC under false oscillation attack.

As shown in the simulation results, due to the false oscillation attack, the WH-PODC provides a wrong response to Area I that causes the frequency oscillation in both connected AC systems. As shown in Fig. 14(a2) and Fig. 14(b2), the frequencies in both

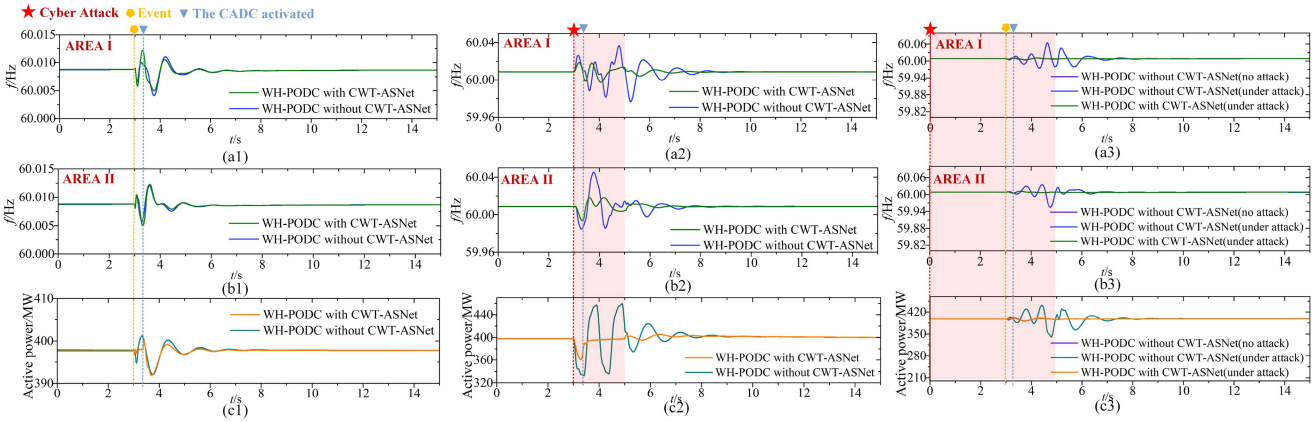


Fig. 14. The performance comparison of improved WH-PODC control framework and traditional WH-PODC under different cyber attack conditions.

Area I and Area II have a large oscillation until $t = 5$ s. After the oscillation attack ends, the oscillation is gradually suppressed by conventional WH-PODC based on the corrected PMU signals. By contrast, with the improved WH-PODC control framework, the proposed CWT-ASNet detects the oscillation attack around $t = 3.3$ s, then the CWT-ASNet sends a signal to CADC, and CADC adopts FEADC to recover the HVDC response according to the CWT-ASNet signal.

From the simulation results it could be seen that the power flow on the HVDC system is corrected timely, and the frequency oscillation in both AC systems is mitigated by their inner generators. After $t = 5$ s, since the false oscillation attack is ended, the CWT-ASNet sends the signal to CADC to activate the second step of FEADC to recover the LFO controllability of the WH-PODC. The simulation results demonstrate that the frequency oscillation is further suppressed with the WH-PODC participation. The completed simulation results indicate that, compared to the traditional control strategy, the improved WH-PODC control framework could significantly mitigate the frequency oscillation caused by false oscillation attacks.

3) Case III: Replacement Attack Test Scenario: Under the initial condition, the power flow on the HVDC system is 400 MW. At $t = 0$ s, the PMU1 and PMU2 are under the replacement attack that swaps the measurement data of the two PMUs. At $t = 3$ s, an AC line trip event occurs between Bus 7 and Bus 8. At $t = 5$ s, the replacement attack is over. The Fig. 14(a3),Fig. 14(b3) and Fig. 14(c3) shows the performance comparison of the improved WH-PODC control framework and traditional WH-PODC under replacement attack.

As shown in the simulation results, At $t = 3$ s, due to the AC line trip event, an oscillation occurs in Area I and Area II. If there is no cyber attack, as shown in the purple line of Fig. 14(a3) and Fig. 14(b3), the frequency oscillations in both areas are mitigated with the conventional WH-PODC. However, as shown in the blue line of Fig. 14(a3) and Fig. 14(b3), due to the replacement attack, the measured data of the PMU1 and PMU2 are exchanged, the WH-PODC provides inverse support to both areas, which acerbates the frequency oscillations in both areas and power oscillations on the HVDC system. With the proposed improved WH-PODC control framework, Around $t = 3.3$ s, the detection results are obtained from the CWT-ASNet and sent to CADC. The CADC adopts DERC to provide the necessary support to both areas according to the CWT-ASNet signal. It can be seen from the simulation results that the frequency oscillations in both areas are quickly mitigated. The simulation results demonstrate that the improved WH-PODC control framework could provide effective LFO suppression support even under the replacement attacks.

VI. Conclusion

In this paper, an improved WH-PODC control framework is proposed to remediate the adverse effect caused by the cyber attacks for wide-area measurement system based high voltage direct current damping control. In the proposed WH-PODC control framework, the CWT-ASNet framework is proposed to identify the cyber attacks. Three different comparative experiments show the CWT-ASNet has 95.53% and 95.60% accuracy for 10 Hz and 120 Hz reporting rates, respectively, even compared with state-of-the-art methods (MM-gcForest and EEMD-FFT-BP). The ASNet also has lower testing time compared with some commonly used CNNs. The performance verification of the improved WH-PODC control framework is verified with three cases in a modified two-area Kunder system in RTDS. The experimental results demonstrate that the proposed WH-PODC control framework could provide effective LFO suppression capability under different types of cyber attacks, reaching similar stability to conventional LFO controls under normal operating conditions.

In future work, the proposed CWT-ASNet and the improved WH-PODC control framework are planned to be implemented on the hardware WH-PODC controller and tested in the HIL environment that mimics realistic operating conditions.

References

[1] T. J. Overbye, "The electric power grid what lurks behind the outlet and why it matters." Accessed: Apr. 22, 2022. [Online]. Available: https://gcep.stanford.edu/pdfs/iq9bO_1Ib0rRuH_ve0A2jA/Overbye-20071101-GCEP.pdf

[2] K. Prasertwong, N. Mithulananthan, and D. Thakur, "Understanding low-frequency oscillation in power systems," *Int. J. Elect. Eng. Educ.*, vol. 47, no. 3, pp. 248–262, 2010.
[3] 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.
[4] W. Li and X. He, "Review of nonisolated high-step-up DC/DC converters in photovoltaic grid-connected applications," *IEEE Trans. Ind. Electron.*, vol. 58, no. 4, pp. 1239–1250, Apr. 2011.
[5] L. Badesa, F. Teng, and G. Strbac, "Optimal portfolio of distinct frequency response services in low-inertia systems," *IEEE Trans. Power Syst.*, vol. 35, no. 6, pp. 4459–4469, Nov. 2020.
[6] K. Sun, H. Xiao, J. Pan, and Y. Liu, "VSC-HVDC interties for urban power grid enhancement," *IEEE Trans. Power Syst.*, vol. 36, no. 5, pp. 4745–4753, Sep. 2021.
[7] L. Huang, H. Xin, and Z. Wang, "Damping low-frequency oscillations through VSC-HVDC stations operated as virtual synchronous machines," *IEEE Trans. Power Electron.*, vol. 34, no. 6, pp. 5803–5818, Jun. 2019.
[8] R. Preece, J. V. Milanović, A. M. Almutairi, and O. Marjanovic, "Damping of inter-area oscillations in mixed AC/DC networks using WAMS based supplementary controller," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1160–1169, May 2013.
[9] Y. Li, C. Rehtanz, S. Ruberg, L. Luo, and Y. Cao, "Wide-area robust coordination approach of HVDC and FACTS controllers for damping multiple interarea oscillations," *IEEE Trans. Power Del.*, vol. 27, no. 3, pp. 1096–1105, Jul. 2012.
[10] 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.
[11] C. Lu, X. Wu, J. Wu, P. Li, Y. Han, and L. Li, "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.
[12] 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.
[13] R. Fan, J. Lian, K. Kalsi, and M. A. Elizondo, "Impact of cyber attacks on high voltage DC transmission damping control," *Energies*, vol. 11, no. 5, 2018, Art. no. 1046.
[14] W. Qiu, K. Sun, W. Yao, W. Wang, Q. Tang, and Y. Liu, "Hybrid data-driven based HVDC ancillary control for multiple frequency data attacks," *IEEE Trans. Ind. Inform.*, vol. 17, no. 12, pp. 8035–8045, Dec. 2021.
[15] W. Yao *et al.*, "Resilient wide-area damping control for inter-area oscillations to tolerate deception attacks," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4238–4249, Sep. 2021.
[16] A. Patel, S. Roy, and S. Baldi, "Wide-area damping control resilience towards cyber-attacks: A dynamic loop approach," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3438–3447, Jul. 2021.
[17] J. F. O'Brien and D. Roberson, "Synchrophasor spoofing detection and remediation for wide-area damping control," *Electric Power Syst. Res.*, vol. 199, 2021, Art. no. 107445.
[18] Y. Zhao *et al.*, "Resilient adaptive wide-area damping control to mitigate false data injection attacks," *IEEE Syst. J.*, vol. 15, no. 4, pp. 4831–4842, Dec. 2021.
[19] Y. Cui, F. Bai, Y. Liu, and Y. Liu, "A measurement source authentication methodology for power system cyber security enhancement," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3914–3916, Jul. 2018.
[20] 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.
[21] I. Perry *et al.*, "Differentiating and predicting cyberattack behaviors using LSTM," in *Proc. IEEE Conf. Dependable Secure Comput.*, 2018, pp. 1–8.
[22] *IEEE Standard for Synchrophasor Data Transfer for Power Systems*, *IEEE Standard C37.118.2-2011 (Revision of IEEE Standard C37.118-2005)*, pp. 1–53, 2011.
[23] C. K. David, E. Sanger, and N. Perlroth, "Cyberattack forces a shutdown of a top U.S. pipeline." Accessed: Apr. 22, 2022. [Online]. Available: https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html
[24] I. G. Macola, "The five worst cyberattacks against the power industry since2014." Accessed: Apr. 22, 2022. [Online]. Available: https://www.power-technology.com/features/the-five-worst-cyberattacks-against-the-power-industry-since2014/
[25] BBC, "Ukraine power cut 'was cyber-attack'." Accessed: Apr. 22, 2022. [Online]. Available: https://www.bbc.com/news/technology-38573074
[26] Y. Cui, F. Bai, R. Yan, T. Saha, R. K. L. Ko, and Y. Liu, "Source authentication of distribution synchrophasors for cybersecurity of microgrids," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4577–4580, Sep. 2021.
[27] 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.
[28] 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.
[29] 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.
[30] Ł. Jedliński and J. Jonak, "Early fault detection in gearboxes based on support vector machines and multilayer perceptron with a continuous wavelet transform," *Appl. Soft Comput.*, vol. 30, pp. 636–641, 2015.
[31] W. Qian, Y. Xiao, and R. Yong, "Spectrum leakage suppression for multi-frequency signal based on DFT," in *Proc. 13th IEEE Int. Conf. Electron. Meas. Instruments*, 2017, pp. 394–399.
[32] X. Deng, "Deep learning model to detect various synchrophasor data anomalies," *IET Gener., Transmiss. Distrib.*, vol. 14, no. 6, pp. 5739–5745, Dec. 2020.
[33] N. Ma, X. Zhang, H.-T. Zheng, and J. Sun, "ShuffleNet V2: Practical guidelines for efficient CNN architecture design," in *Proc. Eur. Conf. Comput. Vis. (ECCV)*, Jul. 2018, vol. 11218. [Online]. Available: https://doi.org/10.1007/978-3-030-01264-9_8
[34] A. G. Howard *et al.*, "MobileNets: Efficient convolutional neural networks for mobile vision applications," Apr. 2017, *arXiv:1704.04861v1*.
[35] X. Zhang, X. Zhou, M. Lin, and J. Sun, "ShuffleNet: An extremely efficient convolutional neural network for mobile devices," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, 2018, pp. 6848–6856.
[36] K. He, X. Zhang, S. Ren, and J. Sun, "Delving deep into rectifiers: Surpassing human-level performance on imagenet classification," in *Proc. IEEE Int. Conf. Comput. Vis.*, 2015, pp. 1026–1034.
[37] C. Herrera, F. Krach, and J. Teichmann, "Theoretical guarantees for learning conditional expectation using controlled odernn," Jun. 2020, *arXiv:2006.04727v1*.
[38] Z. Wang, "Theoretical guarantees of transfer learning," Jul. 2018, *arXiv:1810.05986v2*.
[39] P. Kundur, "Power system stability," in *Power System Stability and Control*. Boca Raton, FL, USA: CRC Press, 2007.

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. From 2017 to 2020, he was also a Visiting Scholar with the University of Tennessee, Knoxville, TN, USA. From 2020 to 2021, he was a Research Associate with the Department of Electrical Engineering and Computer Science, University of Tennessee. He is currently an Associate Research Fellow with Shandong University. He has authored or coauthored more than 50 peer-reviewed technical articles or conference papers. His research interests include the HVDC and MVDC system operation, renewable energy integration and machine learning based power system application. He was the recipient of the Best Paper Award from IEEE IAS I&CPS Asia, ECAI, and the SCEMS 2020.

Wei Qiu (Member, IEEE) received the B.Sc. degree in electrical engineering from the Hubei University of Technology, Wuhan, China, in 2015, and the M.Sc. and Ph.D. degrees in electrical engineering from Hunan University, Changsha, China, in 2017 and 2021, respectively. From 2019 to 2021, he was also a joint Doctoral Student with the University of Tennessee, Knoxville, TN, USA, where he is currently a Research Associate with the Department of Electrical Engineering and Computer Science. His research interests include situational awareness, cyber-security of synchrophasor, power quality measurement, and reliability analysis of power equipment.

Yuqing Dong (Student Member, IEEE) was born in Jiangsu, China, in 1995. She received the B.S. degree in 2017 from Sichuan University, Chengdu, China, where she is currently working toward the Ph.D. degree with the College of Electrical Engineering. She is also a Visiting Scholar with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN, USA. Her research interests include high voltage direct current and power system stability.

Chengwen Zhang (Student Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2015 and 2018, respectively. He is currently working toward the Ph.D. degree with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN, USA. His research interests include microgrid operation and control, large-scale power system dynamics, simulation, data analysis, and protection.

He Yin (Member, IEEE) received the B.S. and Ph.D. degrees in the electrical and computer engineering from the University of Michigan-Shanghai Jiao Tong University Joint Institute, Shanghai Jiao Tong University, Shanghai, China, in 2012 and 2017, respectively. He is currently a Research Assistant Professor with the Center for Ultra-Wide-Area Resilient Electric Energy Transmission Networks, University of Tennessee, Knoxville, TN, USA. His research interests include situational awareness, renewable energy source control, optimization, decentralized control of microgird, and PMU design.

Wenxuan Yao (Senior Member, IEEE) received the B.S. and Ph.D. degrees from the College of Electrical and Information Engineering, Hunan University, Changsha, China, in 2011 and 2017, respectively, and the Ph.D. degree from the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN, USA, in 2018. From 2018 to 2020, he was a Research Associate with Oak Ridge National Laboratory. 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.

Yilu Liu (Fellow, IEEE) received the B.S. degree from Xi'an Jiaotong University, Xi'an, China, and the M.S. and Ph.D. degrees from Ohio State University, Columbus, OH, USA, in 1986 and 1989, respectively. He is currently the Governor's Chair of the University of Tennessee, Knoxville, TN, USA, and Oak Ridge National Laboratory. In 2016, she is elected as a member of the National Academy of Engineering. 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, Virginia Tech, which is currently operated at UTK and ORNL as GridEye. Her research interests include power system wide-area monitoring and control, large interconnection-level dynamic simulations, electromagnetic transient analysis, and power transformer modeling and diagnosis.