This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3078770, IEEE Transactions on Power Systems

Frequency Injection based HVDC Attack-defense Control via Squeeze-Excitation Double CNN

Kaiqi Sun, *Member, IEEE,* Wei Qiu, *Student Member, IEEE*, Wenxuan Yao, *Senior Member, IEEE,* Shutang You, *Member, IEEE,* He Yin, *Member, IEEE,* Yilu Liu, *Fellow, IEEE*

***Abstract*—Due to the independent controllability and fast power regulation capability, the High Voltage Direct Current (HVDC) system could be a prospective technology to provide multiple ancillary services to the system besides conventional bulk power transmission. However, with the increase of False Data Injection Attacks (FDIAs) on PMU data, the HVDC system could have the wrong response once the collected data that the HVDC system relied on is attacked, thus threatening the system operating security. How to ensure the security of the PMU-based HVDC ancillary service control become an urgent issue. To mitigate the risk, this paper proposed an HVDC attack-defense control based on the FDIAs detection method. Firstly, the Squeeze-Excitation based Double Convolutional Neural Networks (SE-DCNN) is proposed to realize fast identification of the attacking frequency type based on the time and frequency domain signals. The duration time of FDIAs is detected by the local outlier factor. Then, utilizing the results from SE-DCNN, HVDC ancillary service control framework is reorganized and an HVDC attack defense control is proposed for suppressing the potential influence of various types of FDIAs on the HVDC system ancillary service. Different experiments results demonstrate that the proposed method has the ability to significantly mitigate the frequency deviation and oscillation under the FDIA.**

***Index Terms*—HVDC ancillary service control, False Data Injection Attacks, Squeeze-Excitation based Double Convolutional Neural Networks, HVDC attack-defense control**

I. Introduction

In the last decade, High Voltage Direct Current (HVDC) systems witnessed a continuous increase around the world with the development of advanced power electronic technology [1], [2]. In the United States, HVDC systems have been successfully used as a good solution to transmit power over long distances and connect independently all three interconnections together [3]. With the development of power electronic technology, such as Voltage Source Converter (VSC) technology, the functionality of the HVDC system has been significantly extended [4].

The HVDC system has the independent controllability of active and reactive power [5]. Thus, besides the long-distance bulk power delivery, the HVDC system could also provide a quick dynamic response to various system disturbances to further the HVDC system and creates additional values. In the United States, a lot of work done by the industry and academia have investigated the benefits of the ancillary service sharing via the HVDC system [6]. For example, the Pacific Northwest National Laboratory explored the reliability service sharing using HVDC networks in the U.S. power grid [7]. These study results indicated that ancillary service sharing is expected to be one of the high-value products provided by the HVDC system to its connected power grids.

The ancillary services of HVDC systems, such as frequency-response sharing, inertial emulation, and damping oscillation response, are realized by real-time HVDC Ancillary Service Control (HASC). Due to the requirement of the real-time information for HASC, wide-area measurement devices, such as Phasor Measurement Units (PMUs), have become essential in the HVDC system control. Recent research activities have utilized PMUs in HVDC real-time control [8], [9]. In the south power grid of China, a wide-area adaptive damping control system through the modulations of multiple HVDC interties was developed [8]. The field test results in the reference [8] show that the commission of a wide-area adaptive damping control system could increase the damping ratio of the dominant modes by more than 10% . This indicates the combination of the PMUs and the HVDC system could bring a significant improvement to the system stability. In North America, the Sandia National Laboratory developed a damping controller, which utilizes a pre-defined control scheme and real-time PMUs communication to modulate the power flow on the HVDC system for inter-area oscillation damping. The controller has been successfully implemented on the pacific DC intertie and has achieved improvement on the system oscillation damping [9].

However, with the increase of cyber attacks on PMUs, ensuring the reliability of the PMU-based HASC is becoming challenging [10], [11]. In normal operation, the fast power regulating rate of the HVDC system is an important advantage for ancillary service. But if the PMU is under cyber attack, the fast regulating capability of the HVDC system will be a

Manuscript received August 17, 2020; revised December 19, 2020 and February 01, 2021; accepted April 25, 2021. This work is supported primary by the National Natural Science Foundation of China under Grant 51777116, and in part by the Postgraduate Scientific Research Innovation Project of Hunan Province under Grant CX20200426. Paper no. TPWRS-01399-2020. *(Corresponding author: Wei Qiu.)*

K. Sun is with the School of Electric Engineering, Shandong University, Jinan, Shandong 250061, China (email: ksun8@utk.edu).

W. 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).

W. Yao is with the College of Electrical and Information Engineering, Hunan University, Changsha 410082, China (e-mail: wenxuanyao@hnu.edu.cn).

S. You, and H. Yin are with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN, 37996, USA (email: syou3@utk.edu, hyin8@utk.edu).

Y. 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 (email: liu@utk.edu).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3078770, IEEE Transactions on Power Systems

disaster to the system operation, for example, the regulating direction is totally reversed from the system actual requirement. Owing to the serious threats to the system operating safety by the cyberattack, some researches have investigated the coping strategies for mitigating the influence [12]–[14]. For example, a framework for cyber-physical DC microgrid False Data Injection Attacks (FDIAs) detection is presented by identifying the unusual change in inferred candidate invariants sets [12]. The hybrid automaton of a DC microgrid shows that the proposed method could obtain candidate invariants and identify FDIA. In [13], a new cyber-physical architecture is proposed for the DC microgrid. The proposed architecture adopts the separating data plane from the network control plane and performing control plane to against cyber attack in the DC microgrid. Compared with the other methods, this architecture improves the robustness against Dos attack while also keeping lower information interaction. However, the customized power discussed in [13] is difficult to use in other types of systems. The reference [14] developed a discordant element approach to detect the cyber attack in the DC microgrid based on the attack elements modeling so that improve microgrid stability under the unreliable wireless channel. These existing studies focus on the DC microgrid and cyber-attack detection, the HVDC system application and corresponding coping ancillary strategies have not received much attention.

The challenges of cyber attack detection for the HVDC application include the detection speed and accuracy. Generally, the cyber attack detection methods can be classified into two classes, including the model-based and data-driven methods [15].

Based on the operating condition of the power system, quasi-static or dynamic model-based detection algorithms are used to detect cyber attacks. For example, the least squares estimator can be established for the steady state modeling of the power system [16]. A two-step kalman filters is developed in [17] to detect FDIA in automatic generation control systems. However, model-based methods need substation configuration and even information on the previous state. In contrast, the data-driven method is model-free, in which neither systems parameters nor models are involved in the FDIA detection. In [18], a model-free method based on the Ensemble Empirical Mode Decomposition (EEMD) and Back Propagation (BP) network is proposed to process the attack swapping the PMU data sources. Nevertheless, this method is time-consuming because the EEMD requires multiple decomposition operations. The spoofed synchrophasor data is detected based on the gcForest with the single replacement attack [19]. Two types of cyber-attacks are simulated to improve the DC microgrids performance [14]. Combines with the Bayesian algorithm, the approximated filter is used in [20] to enhance the resilience of WAMS. However, the selection of the prior distribution will introduce subjective errors in the Bayesian algorithm. Some other data-driven methods, such as Support Vector Machines (SVMs) [21] and Extreme Learning Machine (ELM) [22] have also been proposed for FDIA detection. However, the statistical features need to be designed, such as the correlation and sparsity value [19], [21], which increases the time cost of the method design. This is because that different numbers and combinations of features are needed to be tuned and adjusted to obtain better accuracy. These data-driven methods can learn the characteristics of the attack signal, but their feature extraction ability is limited and may not suitable for dealing with multiple different types of attack signals.

Apart from the above methods, due to the strong feature learning ability of deep learning, it has a greater potential to be used for attack detection in the HVDC system ancillary service control. For example, a recovery strategy is developed to reclose the tripped transmission lines at the optimal reclosing time based on the deep reinforcement learning framework [23]. Simulation results indicate this strategy could minimize the influence of the cyber attack under different scenarios. A security management system that adopts a dynamic neural network to detect the cyber attack with the concept of residual generation is proposed in [24]. Next, [25] and [26] utilized Deep Reinforcement Learning (DRL) methods to identify the coordinated topology attacks and data integrity attacks, respectively. Simulation results show that the deep reinforcement learning methods obtain profound performance. The input of DRL requires information, including system topology, outputs of generators, and loads, which limits its application. The multi-view Convolutional Neural Network (CNN) is proposed in [27] to detect the spoofing data and source authentication, but it cannot distinguish the type of attack due to the occupation of output labels. The above researches indicate the strong learning ability and accuracy of the deep learning methods in the power system applications, which makes it a potential tool for detecting cyber attacks in the HVDC system ancillary service control. However, the accuracy of deep learning is still constrained by the diversity of input information, in which single information can easily lead to over-fitting and limited adaptability. Meanwhile, the simulated data is used in some research, such as different data-injection scenarios is simulated using the IEEE 39-Bus system [28]. Compared with the simulated data and the actual data, the components such as the noise level and frequency components are different, and the actual data is closer to the real FDIAs.

In this paper, an HVDC attack-defense control based on the deep learning detection method is proposed for suppressing the potential impact of a cyber attack on the HVDC system ancillary service. The contributions of this paper could be summarized as

1) To realize the fast and accurate NFDIA detection, a novel fusion Double Convolutional Neural Networks (DCNN) is proposed. The DCNN can accept two inputs, including the time domain and frequency signals, with improved attack detection performance.
2) To mitigate the interference of redundant information and highlight important features for attack detection, the Squeeze-Excitation (SE) is integrated into DCNN to form the SE-DCNN, which can fully integrate and filtered the extracted time and frequency features.
3) To reduce the NFDIAs impact on the HVDC ancillary control, a frequency injection based HVDC attack-defense control with three control strategies is developed.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3078770, IEEE Transactions on Power Systems

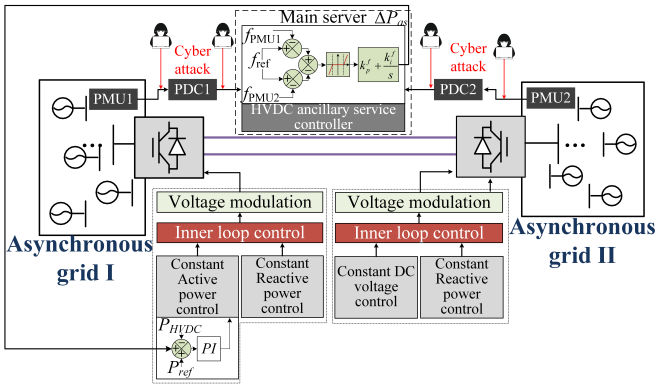


Fig. 1. The control framework of the traditional PMUs feedback based HASC, where f_{ref} is the nominal frequency of the system, P_{ref} is the power order of the HVDC system operator and P_{HVDC} is the measured power flow on the HVDC system.

The proposed HVDC attack-defense control is specifically designed based on the identified type and location of the attack signal in order to suppress the frequency deviation. Different experiments based on actual PMU data are carried out to verify the effectiveness of this framework.

The rest of the paper is organized as follows. The conventional HVDC control framework is introduced in Section II. The steps of SE-DCNN is described in Section III. The reorganized HASC framework is introduced in Section IV. The SE-DCNN based HVDC attack-defense control is presented in Section V. The simulation results are analyzed in Section VI. Finally, the conclusion is given in Section VII.

II. Conventional HVDC Control Framework under NFDIAs

A. PMUs feedback based HVDC control framework

The conventional HVDC ancillary control modulates the power flow on the HVDC system using the PMUs measurements. The control framework of the traditional PMUs feedback based HASC is shown in Fig. 1.

As shown in Fig. 1, the HASC modulates the power flow based on the frequency difference between the points of PMUs measurement. This work process of the frequency response control can be divided into four parts:

1) $Step1$: The frequencies in different asynchronous grids are measured by wide-area PMUs. Generally, the frequency is calculated from the measured voltage phasors [9].
2) $Step2$: The PMUs send the collecting signal to Phase Data Concentrators (PDCs) via User Datagram Protocol (UDP) or TCP/IP protocol. The data packet is sent to PDC via communication protocol IEEE C37.118 [29].
3) $Step3$: After receiving the frequency data, the HASC calculates the frequency difference Δf, between two PMU-measured frequency data. Then the Δf is converted to power modulation order ΔP_{as}, by passing the gain module and sending to basic converter control. The calculation of ΔP_{as} can be expressed as:

$$\Delta P_{as} = [(f_{ref} - f_{pmu1}) - (f_{ref} - f_{pmu2})] \left(k_p^f + \frac{k_i^f}{s} \right) \quad (1)$$

where f_{pmu1} is the frequency measured from PMU1 and f_{pmu2} is the frequency measured from PMU2, the s is differential operators, k_{pf} and k_{if} are proportional gain and integral gain, respectively.
4) $Step4$: The calculated ΔP_{as} is added on the constant active power control to modulate the power flow of the HVDC system, realizing the frequency response function.

B. The risk of cyber attack in the HVDC system

In different structures that the HASC relies on, the PMUs can be maliciously penetrated by cyber attackers due to the vulnerability of its communication protocol [30]. Various methods for cyber attacks can be sorted into three categories: network-based attacks, communication-based attacks, and physical-based attacks [31].

For example, the GPS spoofing is a kind of physical-based attacks where its timestamp reference of PMU measurements can be modified [32]. The radio frequency (RF) jamming belongs to the communication-based attacks, this attack affects the bandwidth sharing capabilities and the network range. The adversary should obtain communication link permissions or be in proximity to the physical device so that causing adverse effects for communication based and physical attacks [15]. For the communication-based attacks, the entire network may be attacked once the permissions of the protocol are obtained [15]. Besides, the Denial-of-Service attack can also shut down a machine or network, making it inaccessible to its intended users. However, the network-based FDIA is possible from anywhere once the adversary gets access to one of the nodes of the network in the power system since the transfer protocol IEEE C37.118 lacks security mechanisms and confidentiality [15]. Thus, this kind of attack is relatively difficult to defend, and it is likely to have a large impact on the control of HVDC.

Fig. 1 depicts the cyber attack concept of the NFDIA in the HASC. As shown in Fig. 1, the NFDIA can be implemented between the PMUs and PDCs or between the PDCs and HASC controller, so as to deceive HASC and cause false control. Owing to the malicious influence of the NFDIA, the number of NFDIA incidents may significantly increase. Thus, the frequency injection attack based defending strategy becomes an urgent requirement for the HVDC system.

III. NFDIA detection using SE-DCNN

A. NFDIA detection Framework

To improve the HVDC control performance under different frequency injection attacks, the classification and time location of NFDIA is the prerequisite. It is founded that the frequency or statistical features are extracted for false frequency data identification in some advanced methods [18], [33]. However, the complexity of NFDIA will weaken the recognition performance because the manual attacks are often more secretive.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3078770, IEEE Transactions on Power Systems

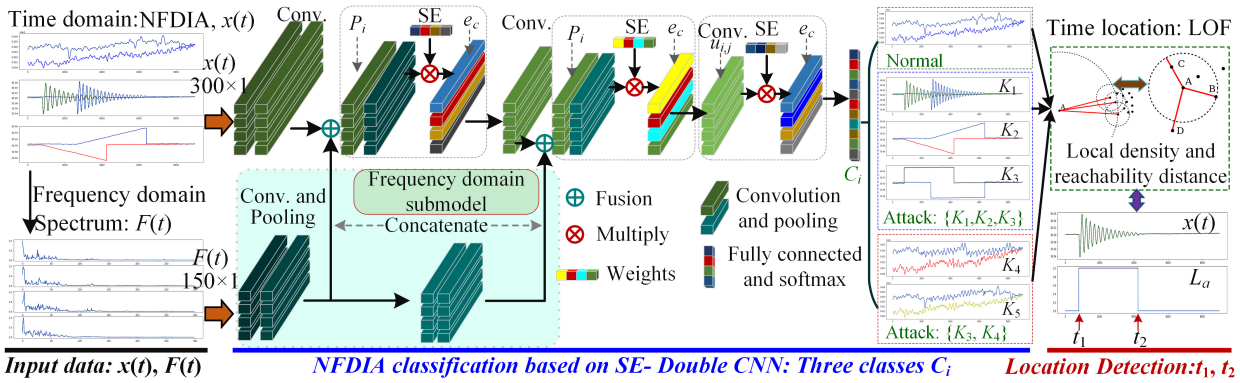


Fig. 2. The framework of FDIA detection based on SE-Double CNN.

To address this issue, a Squeeze-Excitation based Double Convolutional Neural Networks (SE-DCNN) is proposed, whose framework is depicted in Fig. 2. Compared with some deep learning methods, such as the stacked autoencoders [34], the designed DCNN can accept two inputs, including the time domain and frequency signals. This means more information can be used to determine the attack signal, thereby improving accuracy. Meanwhile, the advantage of SE is that higher weights will be assigned to the features that are useful for cyber-attack detection.

Given the measurement frequency data as $x(t)$, this framework contains three steps as shown in Fig. 2.

1) *Input data preparation.* The spectrum of $x(t)$ is calculated as $F(t)$ through fast Fourier transform, the input becomes the combination of raw data and spectrum $\{x(t), F(t)\}$.
2) *Classification using NFDIA.* The double input structure is designed and then the $\{x(t), F(t)\}$ are fed to SE-DCNN. The frequency domain submodel is used to extract the frequency features from $F(t)$. The substructure of $x(t)$ is responsible for feature extraction and feature fusion. The SE is embedded behind each convolutional layer to filter features. Then, the NFDIAs are divided into three classes $C_i, i = 1, 2, 3$ for better HVDC control, including the normal data C_1, fake event NFDIA C_2, and interchange NFDIA C_3 class.
3) *Time location detection.* The Local Outlier Factor (LOF) is used to detect the location of the false data based on the raw data $x(t)$. The duration of the attack is treated as abnormal data, where the consecutive points at the beginning and end can be seen as the start and end time of the attack. The time is recorded as t_1 and t_2.

In this paper, five types of NFDIAs with different characteristics are selected, including the false oscillation attack (K_1), ramp attack (K_2), scale attack (K_3), data interchange attack (K_4), and playback attack (K_5). Compared with several limited types of cyber attacks in [21], [35], less than three types of attacks are simulated to verify the detection or the control effectiveness of FDIA in the real PMU data streams and DC Microgrids, respectively. Here, different control strategies are designed to defend against cyber attacks in the HVDC system so that more FDIAs are considered. If an unknown attack appears and its impact on the system is similar to scale attack and ramp attack, then it can also be classified as the same major category. This means that the impact of unknown attacks on the HVDC control system will be highly reduced.

Different from some of the aforementioned literature, the actual PMU data based simulated attack signals are used, which will be closer to the real attack. Additionally, the time location of the FDIA can be detected, which will improve control response of HVDC ancillary. The purpose of selecting $K_1, K_2,$ and K_3 is to create a false power system event such as forced oscillation and generation trip. Similarly, the purpose of selecting $K_4,$ and K_5 is to cover up the ongoing disturbance and thus avoid the system response. Therefore, the $\{K_1, K_2, K_3\}$ and $\{K_4, K_5\}$ are classified into the fake NFDIA event class and interchange NFDIA class during the HVDC defense control, respectively.

B. Structure of SE-DCNN

The CNN has strong feature extraction ability, where the deep and number of parameters can be adjusted. Typically, the CNN consists of the convolutional layer, Max Pooling Layer (MPL), and Fully-Connected Layer (FCL) [27]. Feature mapping and learning are primarily done through the convolutional layer. The dimension compression of the learned NFDIA features is performed by MPL. The FCL is used for the NFDIA feature classification. In traditional CNN, only one input is used, which limited the amount of input information. To enrich the input information and improve the detected accuracy, the time domain $x(t)$ and frequency domain $F(t)$ are combined and fed into CNN. Therefore, Double CNN (DCNN) is proposed to process the two types of inputs.

In DCNN, the output features from two different MPLs are stitched to form time-frequency domain features. Denoting the extracted time and frequency features of MPLs as $\bar{x}(t)$ and $\bar{F}(t)$, then the output of time-frequency features are

$$P_i = max\{0, f(w_x * \bar{x}(t) + b_x) + f(w_f * \bar{F}(t) + b_f)\} \quad (2)$$

where w_x and w_f are the weights in time and frequency submodes, respectively. The b_x and b_f are the biases. The sign * denotes the convolution operation.

Through the fused feature, the time-frequency features are implemented. It is worth mentioning that the length dimensions of $\bar{x}(t)$ and $\bar{F}(t)$ need to be the same to successfully concatenate. Compared with stitching directly at the input, the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3078770, IEEE Transactions on Power Systems

advantage of this double-channel stitching method is that the source of features is more controllable, and the number of fusions can be adjusted.

However, the contributions of features from the time and frequency domains have not been recognized, which means that some redundant features will be retained. To eliminate this problem, the squeeze-excitation structure is introduced to DCNN and the SE-DCNN is proposed. The SE can then be used to assign a weight to each feature. The advantage of SE is to highlight the useful features and weaken the redundant features, so that the extracted features are beneficial to classification.

The SE mainly increases the convolutional feature sensitivity to informative features by explicitly modelling channel interdependencies [36]. SE helps the model focus on the characteristics of the attack signal instead of some other signals. For example, the scale attack has a larger amplitude jump compared to the normal signal. Therefore, SE will assign this jump feature a higher weight, so that the model can easily distinguish the scale attack. It consists of two steps including squeezing and excitation. In the first step, the global spatial information is compressed to a channel descriptor. Namely, the NFDIA feature in each channel is squeezed into a point with length one, which is achieved by the global average pooling. This process can be expressed as

$$s_c = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} u(i,j) \tag{3}$$

where H, W are the height and width of the features from the previous layer, respectively. The $u(i,j)$ is the data element. If the SE is used after the concatenate operation, then the $u(i,j) \in P_i$. The width can be regarded as $W = 1$ for the one-dimensional convolution.

Next, the excitation is used to adjust channel interdependencies adaptively through weights. This is achieved by the gating mechanism, which can be represented as

$$e_c = u(i,j)\delta(g(s_c, W)) = u(i,j)\delta(W_1\delta(s_c W_2)) \tag{4}$$

where δ denotes the Rectified Linear Unit (RELU) activation function, the W_1, W_2 are the weights of the RELU. The equation (4) shows that the input data element is multiplied by a set of channel factors. It can be also regarded as the self-attention function for all the channel features.

Finally, the softmax function is used as the last layer for the NFDIA classification in SE-DCNN. As shown in Fig. 2, by alternately using SE in DCNN, time-frequency features can be continuously screened and optimized. Thereby increasing the recognition accuracy of different NFDIAs.

C. Location detection of frequency injection attack

For the SE-DCNN based HVDC control to be of practical use, the time location is required to offer real-time control capability. To fulfill this objective, the LOF is used to identify the attacked data location. LOF is an unsupervised method, which can extract attack data information more efficiently by combining SE-DCNN. The LOF tries to find the anomalous data by measuring the local density of data with respect to its neighbors [37]. The advantage of LOF is that it has the characteristics of fast execution speed and high precision. It is the first time to detect the cyber attack location using the LOF.

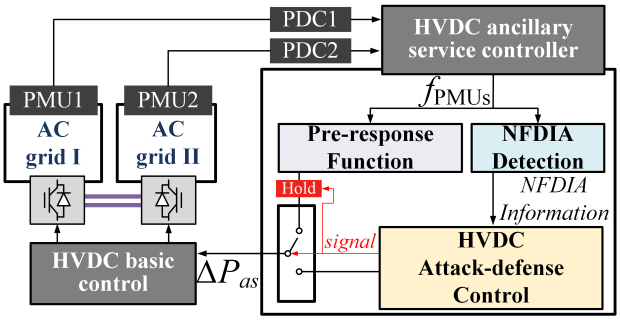


Fig. 3. The reorganized HASC framework.

In LOF, the output label of each data point can be denoted as binary form $l(x) = \{0, 1\}$. When $l(x) = 1$, it means that the corresponding data is an outlier. And the data point is the normal data if $l(x) = 0$. By counting the interval where the label is 1, we can know where the attack occurred. Moreover, to prevent abnormal interference such as the noise, the position with 10 consecutive outliers is deemed as the starting time t_1 of the false injection attack. Similarly, the end time is defined as t_2. Based on this consideration, an Attack Location (AL) indicator is defined to verify the accuracy of location detection, which can be expressed as

$$AL = \frac{\sum l(x) = 1}{L_a} \tag{5}$$

where the total number of data points for the detected results in LOF, L_a is the length of the actual number of attacked data points. Obviously, it shows a better detection accuracy when AL is close to 1. Based on the detection results from the SE-DCNN framework, the efficient HVDC ancillary control can be achieved.

IV. The Reorganized HVDC Ancillary Service Control Framework

Consider the impact of the cyber attack, the control objective of the HASC is shifting from only focusing on the fast response capability to giving the same importance to the response speed and mitigating the impact from a cyber attack. The control objective upgrading of HASC needs a new control approach to better coordinate the multiple functions. In this section, a reorganized HASC framework is introduced. The detailed control framework of novel reorganized HASC is shown in Fig. 3.

As shown in Fig. 3, different from the control framework of conventional HASC, the reorganized HASC framework involves the detection result of a cyber attack into the controller. The reorganized HASC framework could be described as follow:

1) After PMUs measure and send the frequency data to the HASC controller through the PDCs, in the HASC controller, the frequency data is firstly fed into pre-response function and NFDIA detection.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3078770, IEEE Transactions on Power Systems

2) According to the SE-DCNN, the NFDIA detection will determine whether the measured frequency is attacked. If the measured frequency is attacked, the NFDIA detection will also obtain the types and time duration of the NFDIA.
3) The pre-response function is also activated at the same time as NFDIA detection. The pre-response function adopts conventional HASC, as shown in Fig. 1. However, the adopted droop coefficient of the pre-response function, k_{rs}, is smaller than the normal droop coefficient k_p^f in conventional control. Thus, the setting of the droop coefficient in the pre-response function can still realize part of the response performance of the original HASC while avoiding the serious consequence caused by the wrong response of the cyber-attacked HVDC system.
4) When the NFDIA detection is finished, the NFDIA information, which includes whether the HVDC system is attacked or not, the type and the during time of the NFDIA, are delivered to HVDC attack-defense control. The HVDC attack-defense control will hold the response of the pre-response function first, and then use the NFDIA information to adopt suitable response control strategies to provide correct ancillary service to the system.

The detailed control strategies of the HVDC attack-defense control is introduced in Section V.

V. HVDC ATTACK-DEFENSE CONTROL VIA SE-DCNN

Traditionally, the HASC is hard to balance the fast response requirement and cyber attack defending due to the limitation of the detection method. When the attack occurs, they can only freeze the HASC in tens or hundreds of milliseconds to wait for recovery. To achieve efficient control, this paper proposes an HVDC attack-defense control based on the detected types and duration time of NFDIA from SE-DCNN. The HVDC attack-defense control is expected to break through the detection restriction and provide another train of thought to guarantee both response speed and control safety.

The objective of the proposed HVDC attack-defense control is to provide fast and effective power support to the system. The HVDC attack-defense control is based on the detecting results from SE-DCNN. According to the classification of the SE-DCNN, the NFDIA can be classified into the normal data C_1, fake event NFDIA C_2, and interchange NFDIA C_3. For each type of NFDIA, a specific response strategy has been designed in the HVDC attack-defense control system based on the attack detecting time and end time (t_2) detected from NFDIA. The detailed control strategies of HVDC attack-defense control are depicted in Fig. 4.

As shown in Fig. 4, the NFDIA detection receives the results from SE-DCNN including C_i, t_1 and t_2, according to the types and time location of NFDIA, C_i, t_1 and t_2 are delivered to the HVDC attack-defense control for realizing different HVDC response to different types of FDIAs. Then, three control strategies are defined in the HVDC attack-defense control according to the SE-DCNN classification results (C_i): Normal Recovery Control (NRC), Event Recovery Control (ERC), and Interchange Recovery Control (IRC).

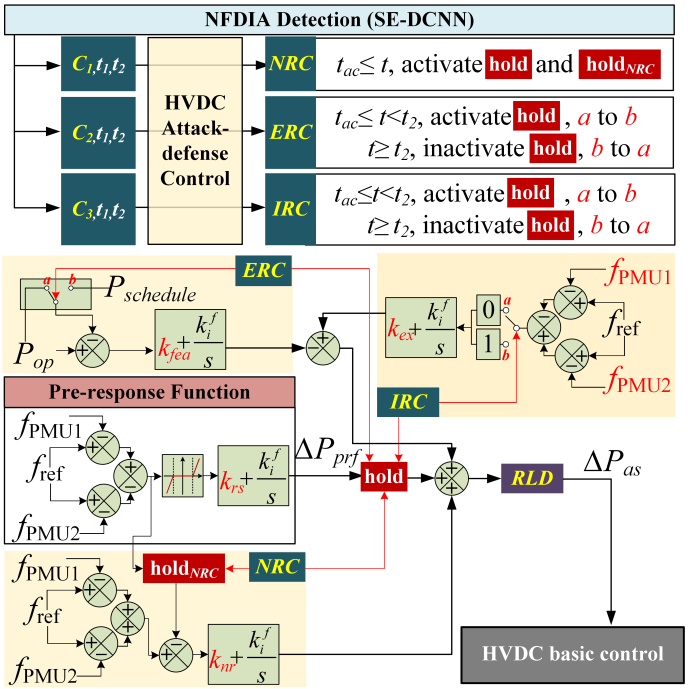


Fig. 4. The control strategies of HVDC attack-defense control, $P_{schedule}$ is the schedule power flow on the HVDC system, P_{op} is the operating power flow on the HVDC system, k_{nr} is the droop coefficient used in NRC, k_{fea} is the droop coefficient used in ERC, the k_{ex} is the droop coefficient used in IRC, t_{ac} is the activated time of the HVDC attack-defense control and the RLD is the rate limiter dynamic in order to avoid the power output pulse.

When the type of NFDIA is C_1, NRC is activated. The objective of NRC is to recover the HVDC response capability to normal HVDC response capability in order to provide appropriate power support to the system. The control process of the NRC could be described as:

1) When the NRC is activated, the NRC sends a signal to the module "hold" to freeze the output of the pre-response function.
2) Meantime, the NRC sends a signal to the module "hold$_{NRC}$" to freeze frequency deviation. Then, the current frequency deviation is fed into NRC to obtain the power modulation order, in order to recover the frequency response capability of the HVDC system back to the normal level.

The ERC is designed to realize a fast system recovery from the wrong HASC of the HVDC system. The control process of the ERC could be described as follow:

1) When the type of NFDIA is C_2, the ERC is activated. The ERC will send a signal to the module "hold" to freeze the output of the pre-response function.
2) At the same time of sending the signal to the module "hold", the ERC sends a signal to the switch module to change the switch from a to b in order to adjust the current power flow of the HVDC system back to the scheduled power flow.
3) When the system operating time is over the end time of the NFDIA, the ERC inactivates the module "hold" to release the output while changing the switch from b to a to stop the ERC response.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3078770, IEEE Transactions on Power Systems

The IRC aims at suppressing the effect of the inverse response of the HASC caused by the NFIDA. The inverse response of the HASC may have the worst potential effect on system stability. Thus, the HVDC attack-defense control needs to provide very fast and strong power support to the system in order to correct the frequency trend and stabilize the frequency as soon as possible. The control process of the IRC could be described as follow:

1) If the type of NFDIA is C_3, the IRC is activated. Similar to the ERC, the IRC will send a signal to the module "hold" to freeze the output of the pre-response function.
2) Meantime, the IRC also sends a signal to the switch module in the IRC to change the switch from a to b to activate the IRC response. The disturbance caused by the event and inverse HASC can then be significantly suppressed by the IRC.
3) When the system operating time is over the end time of the NFDIA, the IRC inactivates the module "hold" to release the output while changing the switch from b to a to stop the IRC response.

The proposed NRC, ERC, and IRC provide flexible response control to realize effective HASC under the no NFDIA condition and various NFDIA conditions. With the three control strategies (NRC, ERC, and IRC), the HVDC system could fast correct its wrong output caused by NFDIA, thus significantly reducing the frequency oscillation of the system and stabilizing the frequency as soon as possible.

VI. Experiments and Analysis

To verify the performance of the proposed SE-DENN method and the HVDC attack-defense control, different experiments and simulation are carried out in python and PSCAD/EMTDC separately.

To detect the NFDIA, the frequency data with a sampling rate of 1440 Hz is used. The length of each sample is set to 9000. To speed up the training time, the data is downsampled to 300 data points per sample. Totally 4330 samples are generated for each attack class K_i, of which 60% are used for training, 20% for verification, and the rest for testing. The normal frequency data also participate in training. Attacks with different duration time and different amplitude differences are randomly set for each sample, which the attack model can be referred to [19], [21], [38]. Since the proposed SE-DCNN is a supervised learning method, the models can be trained based on the samples and the corresponding labels.

Once the training process is finished, a label can be predicted based on the input data and different FDIAs can be recognized. For these unknown FDIAs that did not participate in training, the model would also provide a label that best matches its shape and characteristics. It should be noted that the unknown FDIAs most likely be recognized as any kind of attack signal, rather than a normal data because the attack signal is different from the normal signal in the time domain or frequency domain

In the simulation, a reduced INterconexin ELctrica Francia-Espaa (INELFE) project model is developed in PSCAD software to verify the control performance and the practical value.

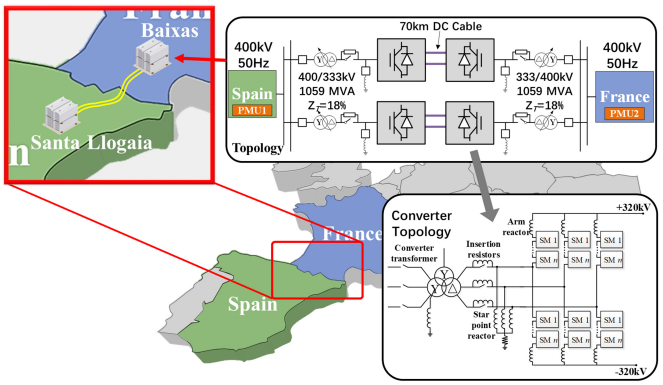


Fig. 5. The topology of the reduced INELFE project

TABLE I
Main Circuit Parameters of the Simulation System

Parameters	Value
Rated powerof MMC/MVA	1000
Nominal voltage of MMC/kV	320
Rated DC current of MMC/A	1562.5
Rated power of Converter transformer/MVA	1050
Nominal voltage of converter transformer/kV	400/333
Leakage impedance of converter transformer/%	18
The inductance of converter reactor/mH	50
Resistance of Insertion resistor/kΩ	5
Inductance of star point reactor/H	5000
Resistance of star point reactor/ kΩ	5
Number of sub-module per valve arm	400
Individual capacitance/mF	10

The topology of the reduced INELFE project model is shown in Fig. 5 [39].

The INELFE project is designed as two identical but independent VSC systems between Spain (Santa Llogaia station) and France (Baixas). The INELFE is composed of 2 HVDC links. Each HVDC link has two MMC terminals. Each phase of the MMC is composed of one upper arm and one lower arm. Each arm is composed of more than 400 sub-modules. Each HVDC link is composed of two symmetrical monopole converters, two step down transformers and two underground cables. The main circuit parameters of the reduced INELFE project model are listed in Table I [40], [41]. In the HVDC system, the Santa Llogaia station is assumed to work at constant DC voltage control, and the Baixas station is assumed to work at constant active power control. In this simulation, two PMUs are adopted as the frequent measurement devices for the HASC, where the PMU1 is configured at the PCC bus of the Santa Llogaia station and the PMU2 is configured at the PCC bus of the Baixas station. The HVDC attack-defense control is configured on the Baixas station to provide power support under the contingency. In the normal operation, the power flow on the HVDC system is 700 MW from Santa Llogaia station to Baixas station.

A. Comparison with advanced methods for SE-DCNN

In the first experiment, the parameters of SE-DCNN are determined through the grid search method. Specifically, three

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3078770, IEEE Transactions on Power Systems

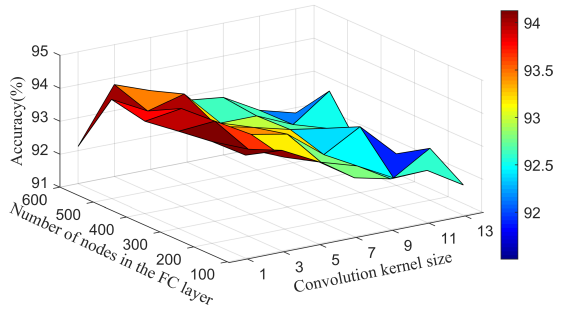


Fig. 6. The accuracy under the different number of nodes in the fully connected layer and convolution kernel size.

TABLE II
SELECTED MODEL HYPERPARAMETERS

Parameters	Values	Parameters	Values
Number of Conv. layers	5	Pooling size	2, 4
Kernel size	3	Dropout rate	0.5
Channels in Conv. layers	16	Batch size	128
Nodes in FC layer	400	92.91	

convolutional layers are used in the frequency domain submodel. Four convolutional layers are used for the time domain submodel. Three SE blocks are used in SE-DCNN as shown in Fig. 2. The kernel size in the convolutional layer is 5. To reduce overfitting, the dropout and Batch Normalization (BN) layer are used in SE-DCNN.

To select the appropriate hyperparameters, this manuscript combines debugging and grid search methods. Here, the convolution kernel size and the number of nodes in the fully connected layer are taken as an example to show how to select the suitable hyperparameters. In this case, the number of nodes in the fully connected layer is set to [100, 600] with step size 100. The convolution kernel size is set to [1, 15] with step size 2. Based on the grid search method, the accuracy is shown in Fig. 6. It can be seen that the accuracy decreases when the size of the convolution kernel increase. The maximum accuracy is at the position where the convolution kernel size is near 1 and 3, and the number of nodes in the fully connected layer is 400. In this way, the selected hyperparameters of SE-DCNN are listed in Table II.

To verify the NDFIA detection performance of SE-DCNN, two advanced methods are used including the EEMD+FFT+BP [18] and MM+gcForest methods [33]. In EEMD+FFT+BP, the FFT results of the decomposition result are fed into BP. Two statistical features are adopted in the MM+gcForest method. The parameters of BP and gcForest are selected using the grid search method. The parameters of BP are selected as 270, and 80 for the first and second layers, respectively. For the gcForest method, the parameters of gcForest are selected as 4 and 2 for the window size and shape of the sample element, respectively. The performance is listed in Table III.

It can be seen that CNN and EEMD+FFT+BP obtain similar accuracy results. However, the EEMD+FFT+BP consumes 590 ms, which is about six thousand times more than CNN. The

TABLE III
PERFORMANCE COMPARISON USING DIFFERENT DETECTION METHODS

Methods	Parameters	Accuracy (%)	AL(%)	Test time (ms)
EEMD+FFT+BP	-	86.85	-	590
MM+gcForest	-	79.53	-	25.9
CNN	280t	84.28	-	0.1
DCNN	310t	93.60	-	6.4×10^{-2}
SE-CNN	303t	91.43	-	1.01
SE-DCNN+LOF	312t	**94.61**	**63.31**	1.03+45.7

-: it is not reported, t: thousands.

reason is that the input of BP only contains the frequency information. The MM+gcForest has the lowest performance due to the limitations of handcrafted features. Compared with the EEMD+FFT+BP and MM+gcForest, both the improved DCNN and SE-DCNN have better accuracy. Compared with CNN, the proposed DCNN improves NFDIA detection accuracy by 9.3%. This is because the DCNN has two inputs, and thereby more information can be learned. And the results of SE-CNN performs 7% higher than the conventional CNN method, indicating the effectiveness of SE. Overall, the proposed SE-DCNN has a profound performance with a 94.61% accuracy. It also demonstrates that SE-DCNN has 10.33% improvement compared with CNN. Compared with CNN and DCNN, the number of parameters for SE-DCNN is only slightly larger. Meanwhile, 46.73 ms is obtained for the proposed framework, indicating that real-time requirements can be met. Only the proposed method has the ability to detect the time location of NFDIA.

When the method is applied to the large scale power system, there would be more types of cyber-attacks and more PMU units data. This also means more redundant features, especially when the network structure increases. In this case, SE will reduce the impact of more redundant features.

To verify the AL detection accuracy, six different types of outlier detection methods are used to verify the cyber attack performance, including kNN, HBOS, LOF, OCSVM, DBSCAN , and LSCP. The AL and test time results are listed in Table IV. HVDC ancillary service control requires fast response time. Therefore, the less detection time means the better. It can be seen that the HBOS consumes less time than the other methods. However, the detection accuracy of AL is also lower than the other methods. The detection time of LOF, and OCSVM can also meet the HVDC control requirements. However, the detection accuracy of OCSVM is inefficient. Based on the detection time and accuracy, the LOF performs better than the other methods.

B. Performance verification of HVDC attack-defense Control

The second experiment is to verify the effectiveness of the proposed HVDC attack-defense control. In this section, the normal operating condition and two different types of NFDIA are used to verify the performance of the proposed HVDC attack-defense control, including the false oscillation

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3078770, IEEE Transactions on Power Systems

TABLE IV
AL PERFORMANCE COMPARISON USING DIFFERENT DETECTION METHODS

Methods	AL Accuracy (%)	Test time (ms)
kNN	52.63	81.25
HBOS	25.17	**26.17**
OSSVM	22.23	65.89
DBSCAN	59.74	92.91
LSCP	36.98	5880
LOF	**63.31**	**45.70**

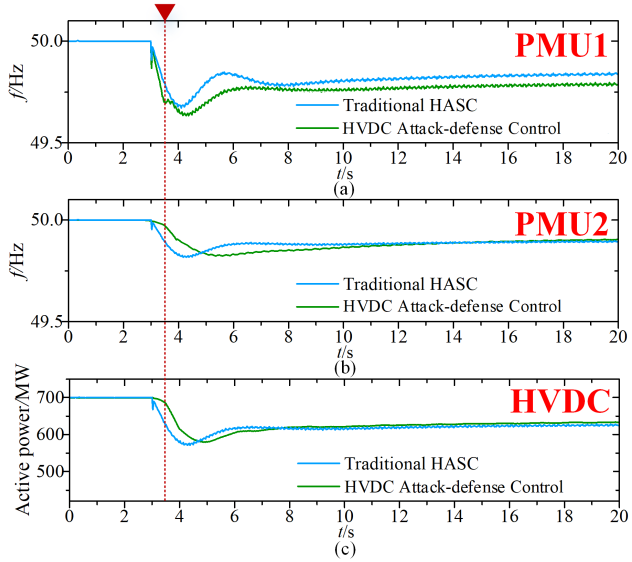


Fig. 7. The performance comparison of proposed HVDC attack-defense control and traditional HASC under no NFDIA condition.

attack (K_1) and data interchange attack (K_4). The NFDIA is simulated according to real oscillation event data.

1) Case I: Normal operating condition test scenario: At $t = 3s$, a generator trip event occurs in the system which the Santa Llogaia station connects. In Case I, a larger delay is set in order to consider other delay caused by various factors. Fig. 7 shows the performance comparison of proposed HVDC attack-defense control and traditional HASC under no NFDIA condition.

As shown in Fig. 7, when the event occurs at $t = 3s$, the proposed SE-DCNN in the NFDIA detection is activated firstly to detect the NFDIA. As can be seen from the simulation results, the function performs of the NFDIA detection may take some time. However, with the proposed NRC, the response of the HVDC system is not significantly influenced because the detection duration is short. The response of the HVDC system is still timely and effective for mitigating the frequency deviation under the contingency.

2) Case II: False oscillation NFDIA test scenario: At $t = 2s$, the PMU1 is under attack with the fake event NFDIA. At $t = 3s$, the PMU1 is attacked with the fake event NFDIA which makes the PMU1 mistake for a fake generator trip event occurs in the AC system that Santa Llogaia station connected. At $t = 6.5s$, the fake event NFDIA is over. Fig. 8 shows the performance comparison of proposed HVDC attack-defense control and traditional HASC under the fake event NFDIA.

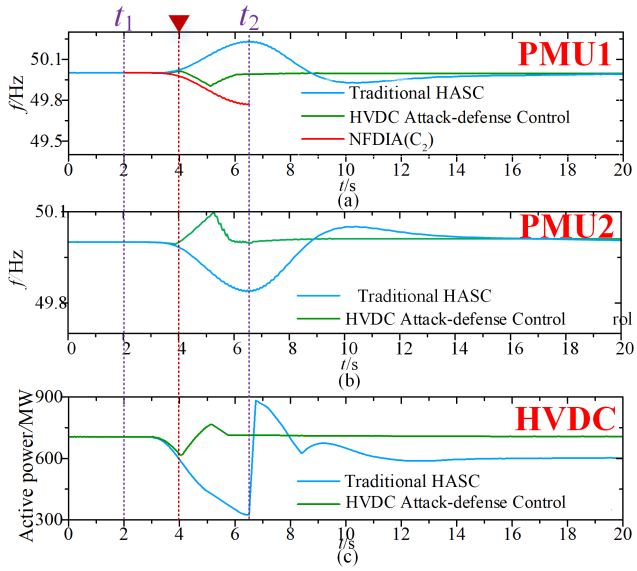


Fig. 8. The performance comparison of proposed HVDC attack-defense control and traditional HASC under the fake oscillation NFDIA.

As shown in Fig. 8, when the fake event occurs at $t = 3s$, the proposed SE-DCNN in the NFDIA detection is activated. At $t = 4s$, the NFDIA is detected, and the ERC is activated. From Fig. 8 (a) and Fig. 8 (b), it could be seen that with the proposed ERC, the frequencies in both systems start to recovery from $t = 4s$. From Fig. 8 (c) could be seen that the power flow on the HVDC system also recovers back to the 700 MW with a constant power regulation rate.

Without the proposed ERC, the traditional HASC of the HVDC system provides a wrong response to the system due to the fake event NFDIA, the frequencies in both systems are significantly affected. Even though the HVDC system starts to provide correct ancillary service after $t = 6.5s$, the influences of the fake event NFDIA are not completely suppressed until the end of the simulation.

3) Case III: Data interchange NFDIA test scenario: At $t = 0s$, the PMU1 is under attack with the interchange NFDIA. At $t = 3s$, a load trip event occurs on the PMU1. At $t = 6.5s$, the interchange NFDIA is over. Fig. 9 shows the performance comparison of proposed HVDC attack-defense control and traditional HASC under the interchange NFDIA.

As shown in Fig. 9, when a load trip event occurs at $t = 3s$, the proposed SE-DCNN in the NFDIA detection is activated. At $t = 3.8s$, the NFDIA is detected, and the IRC is activated. From Fig. 9 (a) and Fig. 9 (b) could be seen that, similar to the ERC, with the proposed IRC, the frequencies in both systems start to recovery from $t = 3.8s$. From Fig. 9 (c), it could be seen that the power flow on the HVDC system is back to the 700 MW.

Without the proposed IRC, due to the interchange NFDIA, the frequency deviation is exponentially amplified with the wrong response of the HVDC system. The frequencies in both systems are significantly affected. Even though the HVDC system starts to provide correct ancillary service in order to mitigate the frequency deviation after $t = 6.5s$, the influences

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3078770, IEEE Transactions on Power Systems

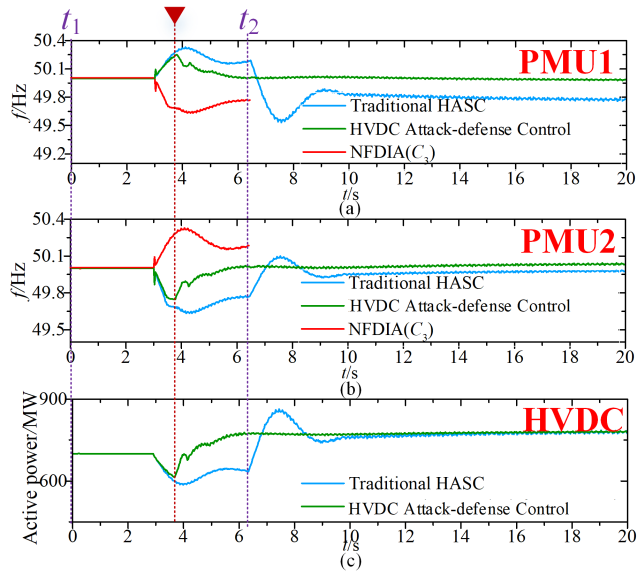


Fig. 9. The performance comparison of proposed HVDC attack-defense control and traditional HASC under the data interchange NFDIA.

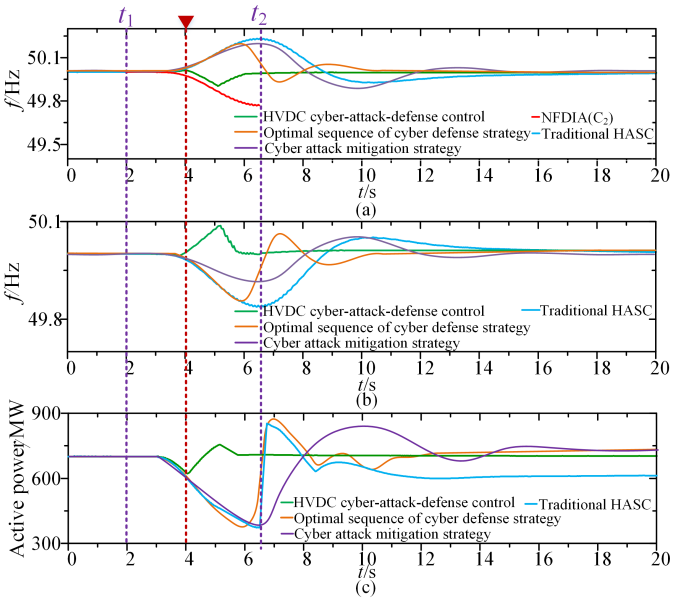


Fig. 10. The performance comparison of proposed HVDC attack-defense control with other advanced defending strategies under the fake oscillation NFDIA.

of the interchange NFDIA persistently exist until the end of the simulation.

Overall, the proposed HVDC attack-defense control could realize similar response performance as the traditional HVDC control performance under the normal condition is acceptable. Under the NFDIA, the proposed HVDC attack-defense control could significantly improve the HVDC cyber attack defense performance. With the verification in a real HVDC project, the proposed HVDC attack-defense control is proved valuable and practical for HVDC cyber attack defense.

C. Comparison of HVDC attack-defense Control

To verify the effectiveness and robustness of the proposed HVDC attack-defense control, the cyber attack mitigation strategy and optimal sequence of cyber defense strategy are adopted to compare the performance of the proposed HVDC cyber attack defense control with other existed defending strategies. In addition, the robust control and decentralized model predictive control are adopted to compare the performance of the proposed HVDC cyber attack-defense control in different control strategies. The control principle of the cyber attack mitigation strategy could refer to [42], the control principle of the optimal sequence of cyber defense strategy could refer to [43], the control principle of robust control could refer to [44] and the control principle of decentralized model predictive control could refer to [45], respectively.

The false oscillation NFDIA test scenario is adopted as the comparison scenario. At $t = 2s$, PMU1 is under attack with the fake event NFDIA. At $t = 3s$, PMU1 is attacked with the fake event NFDIA which makes the PMU1 mistake for a fake generator trip event occurs in the AC system that Santa Llogaia station connected. At $t = 6.5s$, the fake event NFDIA is over. Fig. 10 shows the performance comparison of proposed HVDC attack-defense control and some existing advanced cyber attack defense controls. Fig. 11 shows the performance comparison of proposed HVDC attack-defense control in different HVDC basic control strategies.

As shown in Fig. 10, when the fake event occurs at $t = 3s$, according to the operating principle, the proposed SE-DCNN in the NFDIA detection and the optimal sequence of cyber defense strategy are activated. At about $t = 4.05s$, the NFDIA is firstly detected, and the ERC is activated. At $t = 5.8s$, the NFDIA is detected by the optimal sequence of cyber defense strategy. As can be seen from Fig. 10 (a) and (b) that all three methods can improve the frequency performance compared to the traditional HASC. However, the proposed ERC configured could recover the frequencies in both systems from $t = 4.05s$. The optimal sequence of cyber defense strategy could also detect NFDIA and provide recovery control, but the detecting duration is larger than the proposed SE-DCNN. The cyber attack mitigation strategy could mitigate the frequency deviation in the all simulation process, but the frequency recovery is slower than other methods. The simulation results in Fig. 10 indicate that the proposed HVDC cyber attack defense control could realize better cyber attack defense performance in the NFDIA attack compared to the mentioned existed cyber attack defending methods.

As shown in Fig. 11, when the fake event occurs at $t = 3s$, the proposed SE-DCNN in the NFDIA detection is activated. At about $t = 4.05s$, the NFDIA is detected, and the ERC is activated. From Fig. 11 (a) and (b) it could be seen that, the proposed ERC configured in DLC, RBC and MPC could all recover the frequencies in both systems from $t = 4.05s$. And from Fig. 11 (c), it could be seen that the power flow on the HVDC system also recovers back to the 700 MW. Without the proposed ERC, the HVDC system with either DLC, RBC or MPC will provide the wrong response to the system due to the fake event NFDIA. The frequencies in both systems are significantly affected. From the simulation results, it could be seen that the proposed HVDC attack-defense control is general

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3078770, IEEE Transactions on Power Systems

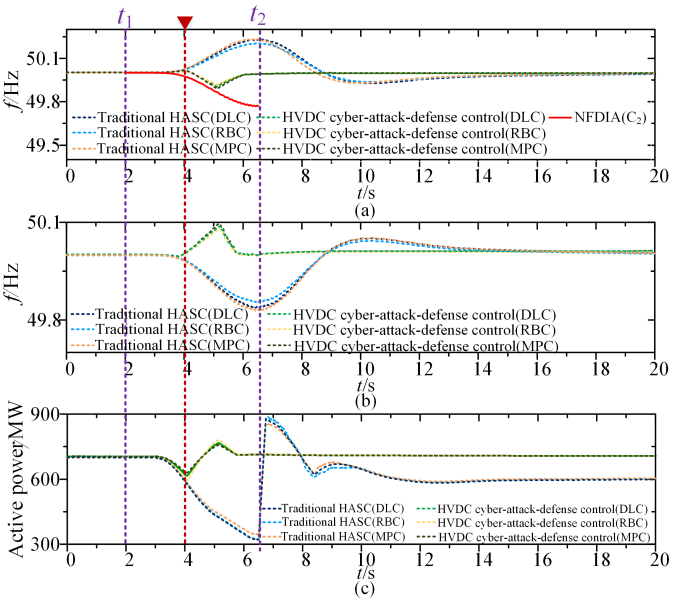


Fig. 11. The performance comparison of proposed HVDC attack-defense control in different HVDC basic control under the fake oscillation NFDIA, where DLC is the traditional double-loop control scheme, RBC is robust control and MPC is decentralized model predictive control.

and could realize good cyber attack defense performance when it is configured in either FPDC, RBC or MPC.

VII. Conclusion

In this paper, a squeeze-excitation based double convolutional neural networks based HVDC attack-defense control is proposed to suppress the influence on the HVDC system caused by FDIAs. The proposed SE-DCNN could identify the attack type and time duration in a short time. The detection result shows that the SE-DCNN has 94.61% accuracy, which is higher than the current advanced methods. Based on the results of SE-DCNN, the HVDC attack-defense control is proposed for suppressing the potential influence caused by NFDIAs on the HVDC system ancillary service. The proposed SE-DENN based HVDC attack-defense control is verified with three cases. The simulation results indicate that the proposed HVDC attack-defense control could provide effective ancillary control to the AC system, thus significantly suppressing the effect of NFDIAs on the HVDC control and improving the operating security of both the HVDC system and AC system. In future work, the detection and defense methods for unknown attacks will be further studied.

References

[1] N. R. Chaudhuri, R. Majumder, B. Chaudhuri, and J. Pan, "Stability Analysis of VSC MTDC Grids Connected to Multimachine AC Systems," *IEEE Transactions on Power Delivery*, vol. 26, no. 4, pp. 2774–2784, 2011.

[2] V. Akhmatov, M. Callavik, C. M. Franck, S. E. Rye, T. Ahndorf, M. K. Bucher, H. Mller, F. Schettler, and R. Wiget, "Technical Guidelines and Prestandardization Work for First HVDC Grids," *IEEE Transactions on Power Delivery*, vol. 29, no. 1, pp. 327–335, 2014.

[3] K. Sun, H. Xiao, L. Sundaresh, J. Pan, K. Li, and Y. Liu, "Frequency response reserves sharing across asynchronous grids through MTDC system," *IET Generation, Transmission Distribution*, vol. 13, no. 21, pp. 4952–4959, 2019.

[4] Z. Yuan, S. You, Y. Liu, Y. Liu, D. Osborn, and J. Pan, "Frequency control capability of Vsc-Hvdc for large power systems," in *2017 IEEE Power Energy Society General Meeting*, 2017.

[5] Z. Liu, K. Li, J. Wang, Z. Javid, M. Wang, and K. Sun, "Research on Capacitance Selection for Modular Multi-Level Converter," *IEEE Transactions on Power Electronics*, vol. 34, no. 9, pp. 8417–8434, 2019.

[6] K. Sun, H. Xiao, J. Pan, and Y. Liu, "A Station-hybrid HVDC System Structure and Control Strategies for Cross-seam Power Transmission," *IEEE Transactions on Power Systems*, 2020.

[7] M. A. Elizondo and H. Kirkham, "Economics of high voltage dc networks," Available: https://certs.lbl.gov/sites/all/files/kirkham-final-hvdc-networks-march-2016.pdf.

[8] 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 *2012 IEEE Power and Energy Society General Meeting*, 2012.

[9] B. J. Pierre, F. Wilches-Bernal, D. A. Schoenwald, R. T. Elliott, D. J. Trudnowski, R. H. Byrne, and J. C. Neely, "Design of the Pacific DC Intertie Wide Area Damping Controller," *IEEE Transactions on Power Systems*, vol. 34, no. 5, pp. 3594–3604, 2019.

[10] A. Sundararajan, T. Khan, A. Moghadasi, and A. I. Sarwat, "Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies," *Journal of Modern Power Systems and Clean Energy*, vol. 7, no. 3, pp. 449–467, 2019.

[11] P. Gomes, "New strategies to improve bulk power system security: lessons learned from large blackouts," in *IEEE Power Engineering Society General Meeting, 2004.*, 2004, pp. 1703–1708 Vol.2.

[12] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of False-Data Injection Attacks in Cyber-Physical DC Microgrids," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 5, pp. 2693–2703, 2017.

[13] P. Danzi, M. Angjelichinoski, . Stefanovi, T. Dragievi, and P. Popovski, "Software-Defined Microgrid Control for Resilience Against Denial-of-Service Attacks," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5258–5268, 2019.

[14] S. Sahoo, J. C. Peng, A. Devakumar, S. Mishra, and T. Dragievi, "On Detection of False Data in Cooperative DC MicrogridsA Discordant Element Approach," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 8, pp. 6562–6571, 2020.

[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 Transactions on Smart Grid*, vol. 11, no. 3, pp. 2218–2234, 2020.

[16] J. Duan, W. Zeng, and M. Chow, "Resilient Distributed DC Optimal Power Flow Against Data Integrity Attack," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 3543–3552, 2018.

[17] M. Khalaf, A. Youssef, and E. El-Saadany, "Detection of false data injection in automatic generation control systems using Kalman filter," in *2017 IEEE Electrical Power and Energy Conference (EPEC)*, 2017, pp. 1–6.

[18] S. Liu, S. You, H. Yin, Z. Lin, Y. Liu, W. Yao, and L. Sundaresh, "Model-free Data Authentication for Cyber Security in Power Systems," *IEEE Transactions on Smart Grid*, pp. 1–1, 2020.

[19] Y. Cui, F. Bai, Y. Liu, P. L. Fuhr, and M. E. Morales-Rodrguez, "Spatio-temporal characterization of synchrophasor data against spoofing attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5807–5818, 2019.

[20] H. M. Khalid and J. C. . Peng, "A Bayesian Algorithm to Enhance the Resilience of WAMS Applications Against Cyber Attacks," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 2026–2037, 2016.

[21] J. Landford, R. Meier, R. Barella, S. Wallace, X. Zhao, E. Cotilla-Sanchez, and R. B. Bass, "Fast sequence component analysis for attack detection in smart grid," in *2016 5th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS)*, 2016, pp. 1–8.

[22] L. Yang, Y. Li, and Z. Li, "Improved-elm method for detecting false data attack in smart grid," *International Journal of Electrical Power & Energy Systems*, vol. 91, pp. 183–191, 2017.

[23] F. Wei, Z. Wan, and H. He, "Cyber-Attack Recovery Strategy for Smart Grid Based on Deep Reinforcement Learning," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2476–2486, 2020.

[24] M. Kordestani, A. Chaibakhsh, and M. Saif, "SMSA Security Management System for Steam Turbines Using a Multisensor Array," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3813–3824, 2020.

[25] D. An, Q. Yang, W. Liu, and Y. Zhang, "Defending Against Data Integrity Attacks in Smart Grid: A Deep Reinforcement Learning-Based Approach," *IEEE Access*, vol. 7, pp. 110 835–110 845, 2019.

[26] Z. Wang, H. He, Z. Wan, and Y. Sun, "Coordinated Topology Attacks in Smart Grid Using Deep Reinforcement Learning," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 1407–1415, 2021.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3078770, IEEE Transactions on Power Systems

[27] 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 Transactions on Smart Grid*, vol. 11, no. 4, pp. 3457–3468, 2020.

[28] H. M. Khalid and J. C. . Peng, "Immunity Toward Data-Injection Attacks Using Multisensor Track Fusion-Based Model Prediction," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 697–707, 2017.

[29] "IEEE Standard for Synchrophasor Data Transfer for Power Systems," *IEEE Std C37.118.2-2011 (Revision of IEEE Std C37.118-2005)*, pp. 1–53, 2011.

[30] I. ALI, M. A. AFTAB, and S. M. S. HUSSAIN, "Performance comparison of IEC 61850-90-5 and IEEE C37.118.2 based wide area PMU communication networks," *Journal of Modern Power Systems and Clean Energy*, vol. 4, p. 487495, 07 2016.

[31] G. Loukas, *Cyber-physical attacks: A growing invisible threat*. Butterworth-Heinemann, 2015.

[32] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 3-4, pp. 146–153, 2012.

[33] Y. Cui, F. Bai, Y. Liu, and Y. Liu, "A Measurement Source Authentication Methodology for Power System Cyber Security Enhancement," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 3914–3916, 2018.

[34] D. Wilson, Y. Tang, J. Yan, and Z. Lu, "Deep Learning-Aided Cyber-Attack Detection in Power Transmission Systems," in *2018 IEEE Power Energy Society General Meeting (PESGM)*, 2018, pp. 1–5.

[35] M. R. Habibi, H. R. Baghaee, T. Dragicevic, and F. Blaabjerg, "Detection of False Data Injection Cyber-Attacks in DC Microgrids based on Recurrent Neural Networks," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, pp. 1–1, 2020.

[36] J. Hu, L. Shen, and G. Sun, "Squeeze-and-Excitation Networks," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2018.

[37] M. M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander, "LOF: Identifying Density-Based Local Outliers," in *Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data*, ser. SIGMOD 00. New York, NY, USA: Association for Computing Machinery, 2000, p. 93104. [Online]. Available: https://doi.org/10.1145/342009.335388

[38] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580–591, 2014.

[39] P. L. Francos, S. S. Verdugo, H. F. lvarez, S. Guyomarch, and J. Loncle, "Inelfe europe's first integrated onshore hvdc interconnection," in *2012 IEEE Power and Energy Society General Meeting*, 2012, pp. 1–8.

[40] S. Dennetire, H. Saad, B. Clerc, E. Ghahremani, W. Li, and J. Blanger, "Validation of a mmc model in a real-time simulation platform for industrial hil tests," in *2015 IEEE Power Energy Society General Meeting*, 2015, pp. 1–5.

[41] S. Dennetière, S. Nguefeu, H. Saad, and J. Mahseredjian, "Modeling of modular multilevel converters for the France-Spain link," *Star*, vol. 2, no. 3, p. 4, 2013.

[42] M. Chlela, G. Joos, M. Kassouf, and Y. Brissette, "Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*, 2016, pp. 1–5.

[43] J. Hou, S. Lei, W. Yin, C. Peng, and Y. Hou, "Optimal cyber defense strategy of high-voltage dc systems for frequency deviation mitigation," in *2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2020, pp. 1–5.

[44] M. M. Belhaouane, M. Ayari, X. Guillaud, and N. B. Braiek, "Robust control design of mmc-hvdc systems using multivariable optimal guaranteed cost approach," *IEEE Transactions on Industry Applications*, vol. 55, no. 3, pp. 2952–2963, 2019.

[45] S. Marithoz, A. Fuchs, and M. Morari, "A vsc-hvdc decentralized model predictive control scheme for fast power tracking," *IEEE Transactions on Power Delivery*, vol. 29, no. 1, pp. 462–471, 2014.

Kaiqi Sun (Member, IEEE) received the B.S. and Ph.D. degree in electrical engineering from Shandong University, Jinan, China, in 2015 and 2020, and was also a visiting scholar with the University of Tennessee, Knoxville from 2017 to 2020. From 2020 to 2021, Dr. Sun was a Research Associate with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN, USA.

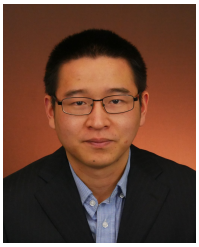
He is currently an Associate Research Fellow with Shandong University. His research interests include the HVDC and MVDC system operation, renewable energy integration and machine learning based power system application. He has authored or coauthored over 50 peer-reviewed technical articles or conference papers. He is the recipient of the Best Paper Award from IEEE IAS I&CPS Asia, ECAI and the SCEMS 2020.

Wei Qiu (Student Member, IEEE) received the B.Sc. degree in electrical engineering from Hubei University of Technology, Wuhan, China, in 2015, and M.Sc. degree in electrical 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 from 2019. His current research interests include power system analysis, cyber-security of synchrophasor, power quality measurement, and reliability analysis of power equipment.

Wenxuan Yao (Senior Member, IEEE) received his 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 in electrical engineering from Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, USA, in 2018. He was a research associate in Oak Ridge National Laboratory 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.



Shutang You (Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Xian Jiaotong University in 2011 and 2014, respectively, and the Ph.D. degree in electrical engineering from the University of Tennessee, Knoxville, in 2017.

He is currently a Research Assistant Professor with the Department of Electrical Engineering and Computer Science. His research interest is in power grid dynamics and monitoring.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3078770, IEEE Transactions on Power Systems

He Yin (Member, IEEE) received the B.S. and Ph.D. degree in the electrical and computer engineering from University of Michigan-Shanghai Jiao Tong University Joint Institute, Shanghai Jiao Tong University, Shanghai, China in 2012 and 2017, respectively. He is currently a postdoctoral researcher at Center for Ultra-Wide-Area Resilient Electric Energy Transmission Networks (CURENT), University of Tennessee, Knoxville, TN, USA.

His research interests include optimization and decentralized control of microgird, and PMU design.

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

Dr. Liu is currently the Governors Chair at the University of Tennessee, Knoxville and Oak Ridge National Laboratory (ORNL). Dr. Liu is elected as the member of 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 at Virginia Tech. She led the effort to create the North American power grid Frequency Monitoring Network (FNET) at 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.