Rapid Monitoring and Defense Approach for Resilience Improvement of Grid Cyber Security

Wei Qiu[1], Yuqing Dong[1], He Yin[1],
[1]*Department of Electrical Engineering & Computer Science University of Tennessee, Knoxville, TN, USA*
qwei4@utk.edu, ydong22@utk.edu, hyin8@utk.edu

Minjun He[2], Buxin She[1], Yilu Liu[1,3]
[2]*University of Bologna, 40136 Bologna, Italy*
[3]*Oak Ridge National Laboratory, TN, USA*
minjun.he@studio.unibo.it, bshe@vols.utk.edu, liu@utk.edu

***Abstract*—False data injection attacks based on synchrophasor measurement data pose a serious threat to the safe and stable operation of power systems. To mitigate this issue, a rapid monitoring and defense approach is proposed to defend against cyber attacks. First, the Time and Frequency based Convolutional neural Network (TFCN) is proposed to detect different types of attacks. In TFCN, the spectrum layer extracts the frequency information of the input data, and then the time-frequency block can be formed. Next, a comprehensive defense strategy is developed for multiple cyber attacks to ensure the stability and resilience of the power system. To verify the effectiveness of the proposed approach, the high-speed frequency measurements collected from the wide-area monitoring system are used. The results demonstrate that the cyber attack detection performance can reach 95.57% compared with traditional neural networks. The defense strategy is conducted and verified in a modified IEEE 39 bus system as well, which shows better performance in faster stability restoration.**

***Index Terms*—Cyber attacks, time and frequency-based convolutional neural networks, comprehensive defense strategy, synchrophasor measurement**

I. Introduction

In recent decades, the potential False Data Injection Attacks (FDIAs) have drawn much attention due to their invisibility and high secretiveness [1]. This malicious impact has penetrated into the power system, automated vehicles, as well as the industrial Internet of Things [2]. For instance, the supervisory control and data acquisition system of Ukraine was hacked in 2015, causing power outages for roughly 6 hours [3]. Besides, 765 trunk line of Venezuela's national grid was attacked, resulting in blackouts in 11 states in 2020 [4]. To enhance the cybersecurity of the power system, it is of great significance to rapidly detect and recover from the adverse effects of cyber attack issues in power system operations.

To detect these attacks, two main methods are used: model-based and model-free approaches. Model-based methods combine the measurements and the power system parameters to find the states and predict the response [5]. Then the abnormal attack phenomenon can be identified by comparing the predicted and actual results. For example, a square-root unscented Kalman filter-based state estimation is constructed to detect the FDIAs in the distribution networks [6]. And an effective and low-cost moving target defense defensive mechanism is developed in [7] to thwart FDIAs. Meanwhile, the minimum number of required distributed flexible AC transmission system devices to protect a specific set of buses is also analyzed. However, obtaining detailed power system parameters and topology poses a significant challenge to the practicality of model-based methods.

In contrast, model-free methods use signal processing techniques for real-time synchrophasor measurements to extract features. Then the traditional machine learning and deep learning methods are used to identify the FDIAs, e.g. robust linear regression and matrix reconstruction [8], [9]. In [10], the mathematical morphological decomposition and multi-weighted deep stacking forest are proposed to achieve accurate source authentication. Next, by exploring the multi-fractal coupling correlations of the synchrophasor measurements, the cost-effective source authentication is conducted [11], which requires the additional procedure of exploring the correlations between the measurements from Phasor Measurement Units (PMUs). Besides, the time-frequency information from the synchrophasor data is extracted first and the effectiveness of the time-frequency information has been verified through the signal processing methods such as synchrosqueezed wavelet transforms and the Hilbert-Huang transform [12], [13]. Then the classifiers are designed to identify the FDIAs, such as the ensemble deep learning [14] and recurrent neural network [15]. Although the FDIAs can be accurately detected by combining signal processing and data-driven-based methods, it is much more time-consuming to optimally select parameters of signal processing methods to extract sufficiently effective features.

So far, some control strategies have already been utilized in modern power systems to defend the potential cyber attacks, most of which focus on the detection algorithms when gathering measurement signals [16], [17]. With the increase of power system complexity, the Wide-area Measurement System (WAMS), taking advantage of the PMUs, requires higher attention due to vulnerable communication and transmission routes. In [18], a time-frequency-based cyber attack defense framework is proposed to achieve fast frequency reserve in a WAMS. Based on the PMU development, the situation is even worse in the distributed energy resource and High Voltage Direct Current (HVDC) systems that are equipped with auxiliary frequency or voltage regulations. Typical solutions can be summarized as control parameter update and

This work is supported by the NSF Cyber-Physical Systems Program (#1931975), and in part by the CURENT Industry Partnership Program.

2023 IEEE Industry Applications Society Annual Meeting (IAS) | 979-8-3503-2016-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/IAS54024.2023.10406496

power reallocation after the detection of cyber attack [19], [20]. Nevertheless, improper control adjustment may have a negative impact on the system's stability and resilience.

To address the above-mentioned limitations, this paper proposes a rapid monitoring and defense approach to improving the resilience of the power grid. The contributions of this paper can be summarized as follows:

1) To achieve the rapid identification of cyber attacks, Time and Frequency-based Convolutional neural Networks (TFCN) is developed, which can achieve the fusion of both the time and frequency domain information without additional spectrum analysis methods.
2) To reduce the impact of cyber attacks, a comprehensive defense strategy is proposed. The cyber attacks are further classified into three categories with corresponding strategies to maintain stability and resilience in power systems.
3) By combining the monitoring and defense approaches, multiple experiments are conducted based on the simulation and actual collected data. Results demonstrate accurate identification of cyber attacks and a high reduction of the negative impact.

II. Proposed Rapid Monitoring Approach of Power Grid Cyber Security

A. Proposed TFCN model

To achieve rapid monitoring and improve the resilience of the power grid, the TFCN is designed firstly, whose structure is demonstrated in Fig. 1. Compared with the traditionally convolutional neural networks, the model has the ability to fuse the frequency domain information directly, and it does not require the additional frequency domain transform such as wavelet transform and Hilbert-Huang transform.

Denoting the input synchrophasor measurements as $x(n)$, a bandpass filter will first filter out the DC component to remove the redundant information. Then it will pass the first convolutional layer to get the deep features $x_1(n)$.

To extract both the time and frequency domain features automatically, the Time-Frequency (TF) block is proposed in TFCN. As demonstrated in Fig. 1, the spectrum will be extracted using the Fast Fourier Transform (FFT). Denoting this process as the spectrum layer, for an N-point data $x_1(n)$, the output of the spectrum layer can be expressed as

$$X(k) = \sum_{n=0}^{N-1} e^{-j\frac{2\pi}{N}nk} x_1(n) \tag{1}$$

Considering that $X(k)$ is the complex form, it is challenging to perform gradient calculations in forward propagation. Therefore, to make the features suitable for the model, only the absolute value of the spectrum layer is preserved, then an additional convolutional layer is connected to the spectrum layer to strengthen the features, which can be calculated as

$$\begin{aligned} O_c(k) &= f(w|X(k)| + b) \\ O_b(k) &= \gamma\left(\frac{O_c(k) - \mu_{\mathcal{B}}}{\sqrt{\sigma_{\mathcal{B}}^2 + \epsilon}}\right) + \beta_b \end{aligned} \tag{2}$$

where the $O_c(k)$ and $O_b(k)$ are the output of the convolutional layer and Batch Normalization (BN) layers, respectively. $f()$ denotes the activation function, and w and b denote the weight and bias of the activation function, respectively. $\mu_{\mathcal{B}}$ and $\sigma_{\mathcal{B}}$ represent the mean and standard error, while β_b and γ are the parameters to adjust the ratio in BN layer.

Thereafter, multiple TF blocks are connected together to strengthen and filter the useful time and frequency features. To make the model converge better, the skip connection is also introduced to the TF block, where its output can be calculated as $O_b(k) + x_1(k)$.

Finally, given the output of the TF block as $O_{bm}(k) = O_b(k) + x_1(k)$, the class of the identified cyber attack results can be simplified and expressed as

$$S_{obm}(m) = \frac{e^{O_{bm}(k)}}{\sum_K \theta_m e^{O_{bm}(k)}} \tag{3}$$

where the m denotes the label of the cyber attacks, and the θ_m denotes the parameter of the softmax function.

After training the model, the real-time synchrophasor measurements can be fed into the TFCN to achieve identification.

B. Feature visualization

To illustrate the feature difference with and without the spectrum information, the features from the convolutional layer are visualized, as shown in Fig. 2. Fig. 2(a) and (b) present the frequency measurement after removing its DC trend component and its frequency spectrum, respectively. The features illustrated in Fig. 2(c) reveal a similar profile with the FFT spectrum, indicating the frequency domain information has been learned. However, the features from (d) are more random because only the time domain information is learned.

In this paper, five types of false data injection attacks are simulated based on numerical models [21], including the normal data ($p1$), noise attack ($p2$), scaling attack ($p3$), replacement attack ($p4$), and false oscillation attack ($p5$).

III. Defense Approach to Improve the Resilience of Power Grid

A. Frequency regulation in VSC-HVDC

After detecting the cyber attacks, the corresponding control strategies can be implemented to defend against their effects. In this case, the HVDC system providing frequency regulation is developed to test the proposed defense approach.

In the conventional control framework of a typical voltage source converter (VSC) based HVDC system, the auxiliary frequency regulation provides additional active power reference value for the HVDC basic control, namely the constant active power control. The inputs of the frequency regulation come from the PMU measurements, f_{PMU1} and f_{PMU2}, at two AC terminals of the VSC-HVDC, which are considered vulnerable to multiple cyber attacks. Basically, the frequency regulation can be expressed as a proportional and integral (PI) control:

$$P_{aux} = (f_{PMU1} - f_{PMU2})\left(k_p + \frac{k_i}{s}\right) \tag{4}$$

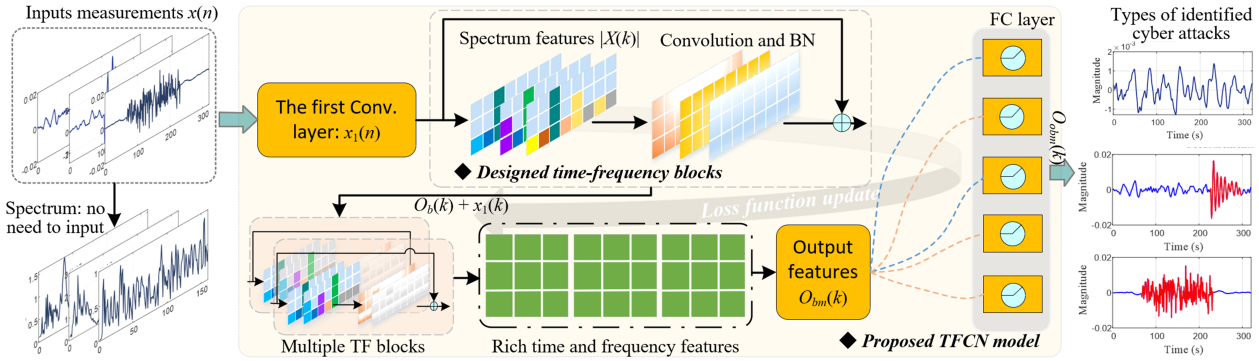

Fig. 1. Framework of the proposed TFCN model.

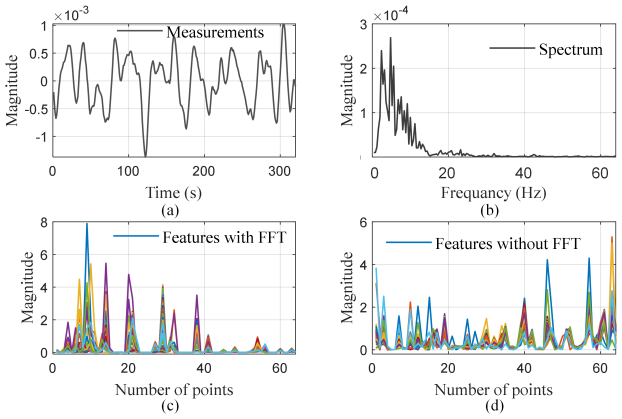

Fig. 2. Feature visualization, (a) frequency measurement after detrending, (b) the spectrum of (a), (c) features of TFCN with TF block, (d) features of TFCN without TF block.

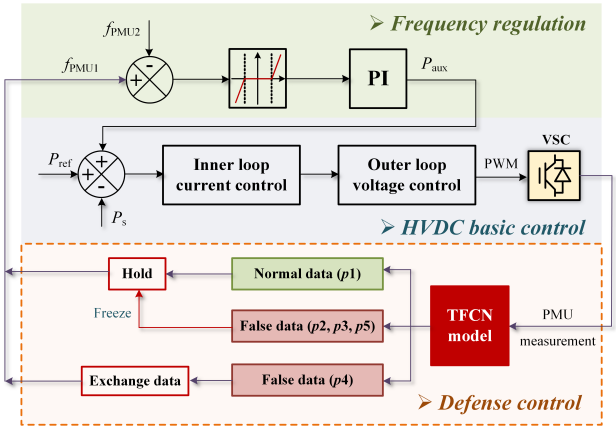

Fig. 3. VSC-HVDC control structure.

where P_{aux} denotes the auxiliary active power output of the frequency regulation; k_p and k_i represent proportional and integral gain, respectively.

By modulating the active power deviation, the inner loop current control and the outer loop voltage control generate the pulse signal to command the switchings inside the VSC converter.

B. Comprehensive defense control strategy

To enhance the resilience of the power system, Fig. 3 depicts the proposed comprehensive defense control strategy based on a VSC-HVDC system. The potential cyber attacks occur during the transmission and communication process of the PMU data collected from AC grids. Accordingly, the TFCN model proposed in II-A is deployed before the PMU signals come into the frequency regulation.

For defense purposes, the five types of false data injection attacks can be further classified into three categories. The noise attack ($p2$), scaling attack ($p3$), and false oscillation attack ($p5$) can be generally considered as false data superimposed on the original data. The control strategies for each false data identification type are demonstrated below.

1) Normal data ($p1$): The normal data can be passed to the frequency regulation without additional processing. On the other hand, it is essential to preserve normal data instantly when the power system is indeed exposed to a cyber attack.

2) False data ($p2$, $p3$, $p5$): The superimposition of false data is quite detrimental as it will directly arouse a power system contingency. To avoid the terrible expansion, the input of the frequency regulation will be frozen to the normal data stored at the last point, as long as the TFCN detects and identifies the cyber attack in this category.

3) False data ($p4$): When a replacement attack is detected, it is quite straightforward to exchange the signals back to their initial measurement locations. Then the data can be sent to the frequency regulation for control purposes. Actually, the replacement attack is harmful when happening along with a power system event, since it will not bring obvious disturbance in steady states.

IV. Experiments

To validate the proposed cyber security monitoring and defense methodology, the off-line TFCN training model utilizes data from three Universal Grid Analyzers (UGAs) with a 120Hz/s high-speed reporting ratio, which are the highly accurate, real-time, and GPS synchronized phasor measurement units [22]. The frequency measurements of UGAs are collected in the FNET/GridEye server located at the University of Tennessee, Knoxville. The dataset consists of 27330 samples and each sample is with a length of 320. During the training, 70% of the dataset is used for training and 30% for testing. Besides, the data collected from the second day is used for verification, which contains 5190 samples. Afterward, the

well-trained TFCN is integrated in a modified IEEE test model for defense strategy verification. Considering that the field data are collected through FNET/GridEye, the generalization of the method can be satisfied.

A. Verification under different parameters

To explore a better performance of the model, the parameters of the TFCN are optimally selected by using grid search. Here, the size of the convolutional layer in the TF block is treated as an example, where the result is listed in Table I. It can be seen that the performance increases from 94.45% to 95.57% when the kernel is lower than 9×1. And the performance decreases when the kernel size is 9×1. Besides, the testing time for each sample is 51.13ms, indicating the real-time performance can be satisfied. In this case, when the window step size of each sample is 10, the corresponding response time is about 134.46ms under a 120Hz reporting rate.

TABLE I
PERFORMANCE OF THE PROPOSED TFCN UNDER THE DIFFERENT SIZES OF CONVOLUTION KERNELS.

Acc. under different size of conv. kernels (%)				Testing time(ms)
3×1	5×1	7×1	9×1	
94.95	95.22	95.57	95.16	51.13

Taking the same parameter optimization method, the primary parameters of the model are listed in Table II. The kernel size 5/7/3 means that the size of the conventional layer at the beginning of the model is 5×1, the kernel near the spectrum layer is 7×1, and the rest is set to 3×1, respectively.

TABLE II
PRIMARY PARAMETERS OF THE TFCN MODEL.

Conv. layers	Kernel size	Nodes in FC	Learning rate	L2
13	5/7/3	256	6e-3	4e-5

B. Performance Comparison of different methods

To verify the robustness of the proposed TFCN model, the loss function value, confusion matrix, and detailed performance are summarized. Based on the optimized parameters, the training loss and the testing loss with and without the FFT spectrum are demonstrated in Fig. 4 under 100 epochs. It can be observed that even though the training loss of the TFCN without the FFT spectrum is lower, the testing loss of the TFCN with FFT is slightly lower. The main reason is that the features of the spectrum increase the complexity of the TFCN model, whereas it has better robustness compared with the TFCN model without FFT.

The detailed performance of each class is presented in Fig. 5. It illustrated that the $p1$, scaling attack, and replacement attack can successfully identify all the samples. However, for the noise attack ($p2$) and false oscillation attack ($p5$), 84.2% and 93.64% accuracies are obtained, respectively. The performance is 2% higher than that TFCN model without

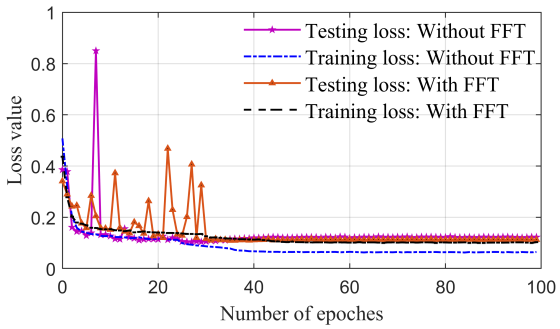

Fig. 4. Training and testing loss for TFCN model with and without FFT spectrum.

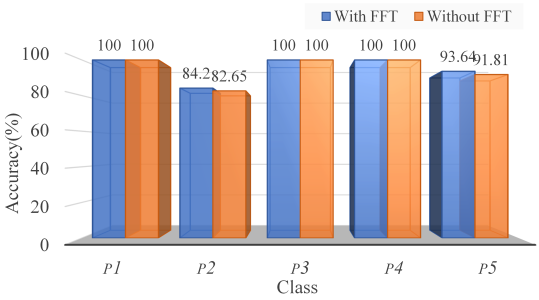

Fig. 5. The detailed performance comparison for each class of cyber attacks.

spectrum, indicating that the spectrum information contributes 2% to the detection of cyber attacks. The main reason is that the frequency measurement is also superimposed with rich noise. And a small part of false oscillation attacks is misidentified.

To further investigate the reason for the misidentification, the confusion matrix is determined, as shown in Fig. 6. As demonstrated in Fig. 6, it reveals that the false oscillation attack and the noise attack are misidentified by each other. When the noise level is higher, and the magnitude of the When the damping coefficient of the oscillation tends to be stable, and when the oscillation frequency is high, the profile of the oscillation and the noise signal are relatively similar.

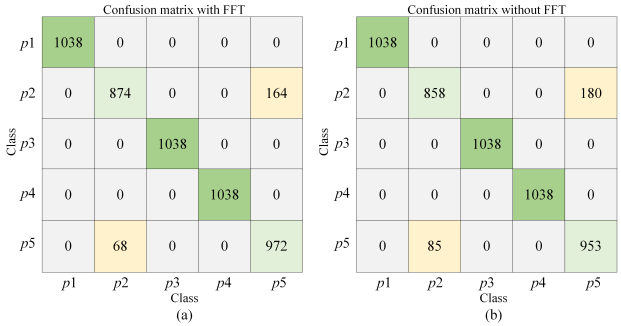

Fig. 6. Confusion matrix results of the TFCN model, (a) TFCN model with FFT, (b) TFCN model without FFT.

C. Cyber Security Defense performance for IEEE test model

To test the performance of the proposed cyber security defense strategy, a modified IEEE 39 bus system is established

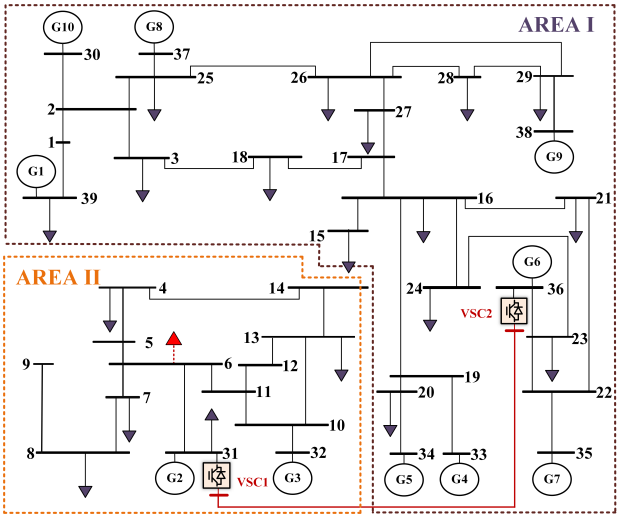

Fig. 7. Topology of modified IEEE 39 bus system.

in PSCAD/EMTDC [23], with a two-terminal VSC-HVDC connecting two split systems, as shown in Fig. 7.

In the test system, VSC1 undertakes the constant DC voltage control, while VSC2 modulates the active power. Therefore, the auxiliary frequency regulation is added at VSC2, with PMU measurements as input from the two terminals. The initial power flow is 20MW transferred from VSC1 to VSC2.

1) Case one: scaling attack ($p3$)

A piece of fake ramping data, $y = 0.8t$, is injected into the PMU at the VSC1 terminal at $t = 1s$.

2) Case two: replacement attack ($p4$)

A load increase of 58MW occurs on Bus 6 at $t = 1s$. Simultaneously, the PMUs measurements from VSC1 and VSC2 are exchanged due to cyber attacks.

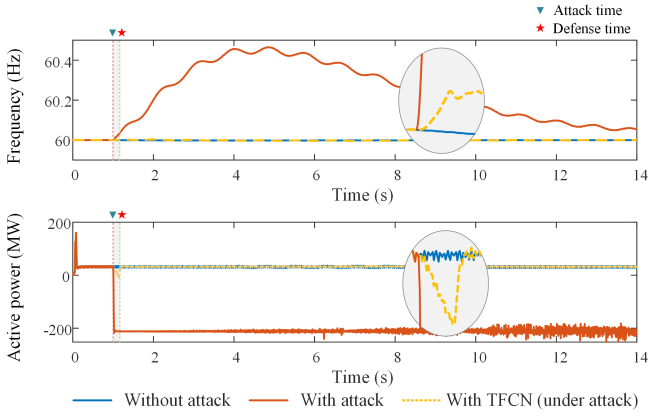

Fig. 8. Frequency and active power performance after scaling attack.

The bus frequency and active power at VSC1 in the above two cases are demonstrated in Fig. 8 and Fig. 9, respectively. The zoomed-in waveforms within the defense time are plotted in the ellipse as well.

For the scaling attack, the negative impact has quite severe behaviors, as shown in Fig. 8. After the PMU measurements are hacked, the bus frequency shows an upward growth with the highest point of 60.42Hz, as well as an inter-area low-frequency oscillation. The active power through HVDC hits the maximum value due to the increasing frequency regulation input. The phenomenon can be fairly harmful without proper management. With the defense strategy integrated, the dynamic performance can be largely improved in terms of both frequency and active power. The frequency deviation along with the oscillation can be quickly eliminated. In addition, the active power only drops 20MW tracking the false frequency within 134.46ms.

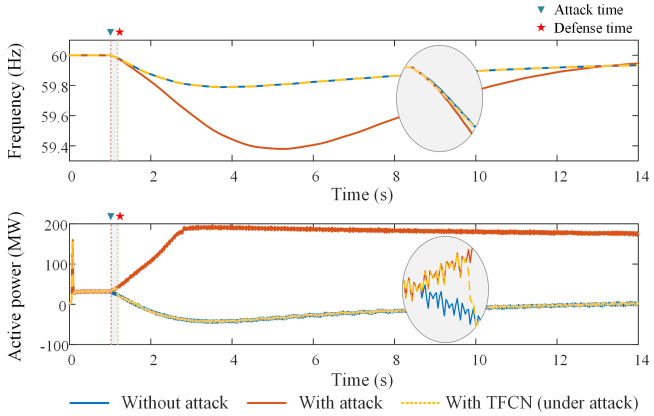

Fig. 9. Frequency and active power performance after replacement attack.

In Fig. 9, the dynamic performance varies much with and without the replacement attack. To be specific, the attack lowers the bus frequency nadir from 59.79Hz to 59.38Hz and extends the frequency restoration time. Meanwhile, the active power of HVDC transmission shows an opposite trend, drastically growing to the maximum power limit of 200MW. With the proposed defense strategy, the bus frequency and active power perform similarly to the circumstances without attack, except for the small disturbance at the very beginning. The excellent results are attributed to the rapid detection and identification of the defense strategy, which corrects the PMU measurements.

V. Conclusions

To achieve rapid monitoring and cyber attack defense, this paper proposes a detection framework based on the time-frequency-based convolutional neural network and the corresponding comprehensive defense strategy. In TFCN, the spectrum layer is fused with the time domain features to avoid additional frequency domain analysis methods. The feature visualization result indicates the frequency features have been learned. The cyber attack detection experiments reveal a 95.57% average accuracy can be achieved. The spectrum information contributes to the performance improvement compared with the TFCN without spectrum. The comprehensive defense experiments in the modified IEEE 39 bus model illustrate that the frequency and active power of the grid can be stabilized quickly. Further research can be developed to distinguish the detailed cyber attacks.

REFERENCES

[1] Z. Ju, H. Zhang, X. Li, X. Chen, J. Han, and M. Yang, "A survey on attack detection and resilience for connected and automated vehicles: From vehicle dynamics and control perspective," *IEEE Transactions on Intelligent Vehicles*, vol. 7, no. 4, pp. 815–837, 2022.

[2] O. Aouedi, K. Piamrat, G. Muller, and K. Singh, "Federated semisupervised learning for attack detection in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 286–295, 2023.

[3] A. Shehod, "Ukraine power grid cyberattack and us susceptibility: Cybersecurity implications of smart grid advancements in the us, [online] available at: https://web.mit.edu/smadnick/www/wp/2016-22.pdf," pp. 1–36, 2016.

[4] D. Du, M. Zhu, X. Li, M. Fei, S. Bu, L. Wu, and K. Li, "A review on cybersecurity analysis, attack detection, and attack defense methods in cyber-physical power systems," *Journal of Modern Power Systems and Clean Energy*, pp. 1–18, 2022.

[5] 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.

[6] S. Wei, J. Xu, Z. Wu, Q. Hu, and X. Yu, "A false data injection attack detection strategy for unbalanced distribution networks state estimation," *IEEE Transactions on Smart Grid*, pp. 1–1, 2023.

[7] Z. Zhang, R. Deng, D. K. Y. Yau, P. Cheng, and M.-Y. Chow, "Security enhancement of power system state estimation with an effective and low-cost moving target defense," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, pp. 1–16, 2022.

[8] J. Tian, B. Wang, J. Li, and C. Konstantinou, "Datadriven false data injection attacks against cyber-physical power systems," *Computers & Security*, vol. 121, p. 102836, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404822002309

[9] H. Yang, X. He, Z. Wang, R. C. Qiu, and Q. Ai, "Blind false data injection attacks against state estimation based on matrix reconstruction," *IEEE Transactions on Smart Grid*, vol. 13, no. 4, pp. 3174–3187, 2022.

[10] Y. Cui, F. Bai, T. Saha, and J. Yaghoobi, "Authenticating source information of distribution synchrophasors at intra-state locations for cyber-physical resilient power networks," *International Journal of Electrical Power & Energy Systems*, vol. 139, p. 108009, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0142061522000540

[11] F. Bai, Y. Cui, R. Yan, H. Yin, T. Chen, D. Dart, and J. Yaghoobi, "Cost-effective synchrophasor data source authentication based on multiscale adaptive coupling correlation detrended analysis," *International Journal of Electrical Power & Energy Systems*, vol. 144, p. 108606, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0142061522006020

[12] W. Qiu, K. Sun, K.-J. Li, Y. Li, J. Duan, and K. Zhu, "Cyberattack detection: Modeling and roof-pv generation system defending," *IEEE Transactions on Industry Applications*, vol. 59, no. 1, pp. 160–168, 2023.

[13] M. Dehghani, M. Ghiasi, T. Niknam, A. Kavousi-Fard, and S. Padmanaban, "False data injection attack detection based on hilbert-huang transform in ac smart islands," *IEEE Access*, vol. 8, pp. 179 002–179 017, 2020.

[14] H. Cui, X. Dong, H. Deng, M. Dehghani, K. Alsubhi, and H. M. A. Aljahdali, "Cyber attack detection process in sensor of dc microgrids under electric vehicle based on hilbert–huang transform and deep learning," *IEEE Sensors Journal*, vol. 21, no. 14, pp. 15 885–15 894, 2021.

[15] J. J. Q. Yu, Y. Hou, and V. O. K. Li, "Online false data injection attack detection with wavelet transform and deep neural networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 3271–3280, 2018.

[16] A. M. Mohan, N. Meskin, and H. Mehrjerdi, "A comprehensive review of the cyber-attacks and cyber-security on load frequency control of power systems," *Energies*, vol. 13, no. 15, 2020. [Online]. Available: https://www.mdpi.com/1996-1073/13/15/3860

[17] T. Huang, B. Satchidanandan, P. R. Kumar, and L. Xie, "An online detection framework for cyber attacks on automatic generation control," *IEEE Transactions on Power Systems*, vol. 33, no. 6, pp. 6816–6827, 2018.

[18] W. Qiu, K. Sun, W. Yao, S. You, and et al., "Time-frequency based cyber security defense of wide-area control system for fast frequency reserve," *International Journal of Electrical Power & Energy Systems*, vol. 132, p. 107151, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0142061521003902

[19] S. Sarangan, V. K. Singh, and M. Govindarasu, "Cyber attack-defense analysis for automatic generation control with renewable energy sources," in *2018 North American Power Symposium (NAPS)*, 2018, pp. 1–6.

[20] K. Sun, W. Qiu, and et al., "Wams-based hvdc damping control for cyber attack defense," *IEEE Transactions on Power Systems*, vol. 38, no. 1, pp. 702–713, 2023.

[21] 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.

[22] L. Zhan, J. Zhao, J. Culliss, Y. Liu, Y. Liu, and S. Gao, "Universal grid analyzer design and development," in *2015 IEEE Power & Energy Society General Meeting*, 2015, pp. 1–5.

[23] Y. Dong, K. Sun, J. Wang, and Wang, "A time-delay correction control strategy for hvdc frequency regulation service," *CSEE Journal of Power and Energy Systems*, pp. 1–11, 2022.