2024 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT) | 979-8-3503-1360-4/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISGT59692.2024.10454172

Data Security Defense: Modeling and Detection of Synchrophasor Data Spoofing Attack for Grid Edge

Wei Qiu[1], He Yin[1], Yuru Wu[1], Chujie Zeng[1]
[1]*Department of Electrical Engineering & Computer Science*
The University of Tennessee, Knoxville, TN, USA
qwei4@utk.edu, hyin8@utk.edu

Chang Chen[1], Yuqing Dong[1], Yilu Liu[1, 2]
[2]*Oak Ridge National Laboratory, ORNL*
Knoxville, TN, USA
liu@utk.edu

***Abstract*—Data security and cyberattack have become critical issues in the distributed power system where adversaries can swap the source information of sensors or even spoof and alter measurements. However, the cyber security of the power system is challenged by the unpredictability and stealth of the spoofing attacks. To protect the data security at the grid edge, this paper developed a synchrophasor data spoofing attack detection framework based on the time-frequency feature extraction techniques including the short-time Fourier transform (STFT) and object detection network for real-time synchrophasor data categorization and spoofing attack localization. The proposed approach outperforms earlier work in terms of spoofing attack detection and offers a vital localization function employing distributed synchrophasor sensors.**

***Index Terms*—Data security defense, synchrophasor data, spoofing attack, time-frequency domain, grid edge**

I. Introduction

The rapid growth of high-penetration renewable energy sources increases the need for real-time monitoring of distributed grid edge. A significant number of sensors, such as the Phasor Measurement Units (PMUs), and smart meters, coordinate with the internet and physical infrastructure to form the heterogeneous Cyber-Physical Power System (CPPS) [1]. The Wide Area Measurement System (WAMS), such as the synchrophasor technologies maintained by the North American SynchroPhasor Initiative (NASPI) and Frequency Monitoring Network (FNET), is a typical CPPS that integrates hardware, software, and application components [2]. However, because of its open compatibility and several flawed protocols, the CPPS has several cyber security problems. Important attack events have caused chaos and significant damage to the power grid in recent years [3]. For instance, an American oil pipeline system suffered a ransomware cyberattack and pipeline operations were halted to contain the attack on May 7, 2021 [4].

Recently, spoofing attacks emerged as a new type of false data injection attack have been reported in some studies [5], [6]. The measurements of the synchronization sensors are susceptible to manipulation, which poses a risk to data-driven applications like oscillation damping control. As a result, the pernicious effects of spoofing attacks promote the necessity of effective means against them and protect data security.

To deal with spoofing attacks in CPPS, numerous efforts have been developed based on system-level techniques. In [7], algorithms based on the linear time-invariant (LTI) system and Kalman filter are studied respectively to defend against cyberattacks. In addition, methods for state estimation and secure control have been developed to address the issue of cyberattacks [8], [9]. However, the common drawback of the aforementioned approaches is the necessity of partial or substantial detailed electrical parameters of the power system, therefore limiting its adaptability.

After that, certain model-free based techniques are developed based on the highly correlated features from the distribution synchrophasors. In [10], the event-unsynchronized and event-synchronized attacks are modeled and the optimization-based attack identification method based on the micro-PMU measurements is proposed [10]. Next, [11] presents a false data injection attack detection method to preserve data privacy using secure federated deep learning. By capturing the unconformity between abnormal and secure measurements, the auto-encoders combined with the generative adversarial network are also intended to fight against the attacks [12]. The typical restriction is that the flexibility of the method will decline since the unique features are not mined.

To mitigate this problem, the multiscale adaptive multifractal detrended fluctuation analysis is proposed to reveal the significant multifractality of the measurements [13]. In response to the data security issue, the continuous wavelet transforms and the convolution neural network (CNN) is connected to authenticating using real-life synchrophasor data [14]. The trials show that it can identify cyberattacks with an accuracy of more than 84 percent while requiring little computational effort. However, the aforementioned methods still have two obvious limitations. The first limitation is that a relatively larger time window (several minutes) of synchrophasor data is utilized [15]. The second limitation is that model-free based approaches such as CNN are unable to determine the localization of the spoofing attack which generates a more considerable delay for data recovery.

To address the above limitations, this paper proposes a practical data security defense solution for synchrophasor data spoofing attacks at the grid edge, of which the contributions

This material was based upon work primarily supported in part by the Engineering Research Center Program of the National Science Foundation and the Department of Energy under NSF Award no. EEC-1041877, and in part by the CURENT Industry Partnership Program and the NSF Cyber-Physical Systems (CPS) Program under Award no. 1931975.

979-8-3503-1360-4/24/$31.00 ©2024 IEEE
Authorized licensed use limited to: UNIVERSITY OF TENNESSEE LIBRARIES. Downloaded on September 20,2024 at 14:26:03 UTC from IEEE Xplore. Restrictions apply.

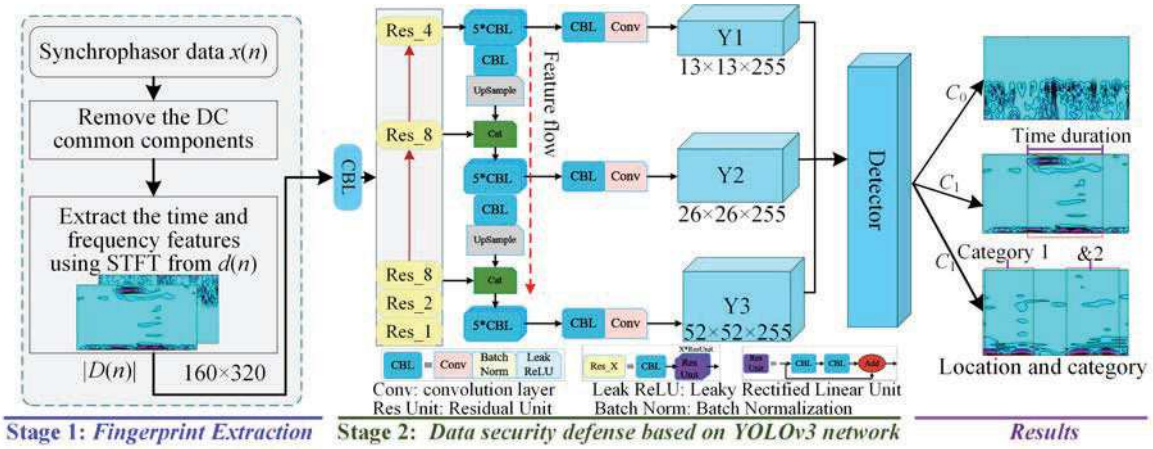

Fig. 1. Proposed data security defense framework based on STFT-based spectrum and YOLO-v3.

can be summarized below:

1) A framework-based short-time Fourier transform (STFT) and You Only Look Once version 3 (YOLOv3) is proposed to perform spoofing attack detection, where the YOLOv3 is a visual analysis algorithm. This data-driven framework has two advantages: it does not need any detailed structure parameters of the grid edge; achieves both the categorization and localization with profound performance.
2) To verify the performance of this framework, the sensitivity of window parameters in STFT, and the comparisons with some state-of-art methods are conducted in detail to explore the feasibility of the algorithm to achieve higher accuracy in practical application.

II. Proposed Data Spoofing Detection Framework

To achieve the synchrophasor data spoofing detection, the data security defense framework based on the STFT-based spectrum and YOLO-v3 is depicted in Fig. 1.

The structure of the proposed framework can be classified into two stages, where the motivation of the first stage is to extract the unique fingerprint information from the measurements using STFT. The second stage is to identify the time duration and category of the spoofing attack using YOLO-v3.

Given the measurement frequency as $x(n)$, as demonstrated in Fig. 2. It reveals that all the synchrophasors have the same DC component σ_{DC} based on their profile. Thus, the common feature needs to be filtered.

Here, a high-pass filter is designed based on the Butterworth filter with a 0.1Hz cut-off frequency. The filtered residual signal $d(n) = x(n) - \sigma_{DC}$ is depicted in Fig. 2(b). It reveals that the DC component has been removed, and the rest useful information as well as the measurement noise are mixed.

III. Time and Frequency Domain Features Extraction using STFT

A. Principle of STFT

Commonly used feature extraction for the non-linearly signals are Empirical Mode Decomposition (EMD) and Ensemble

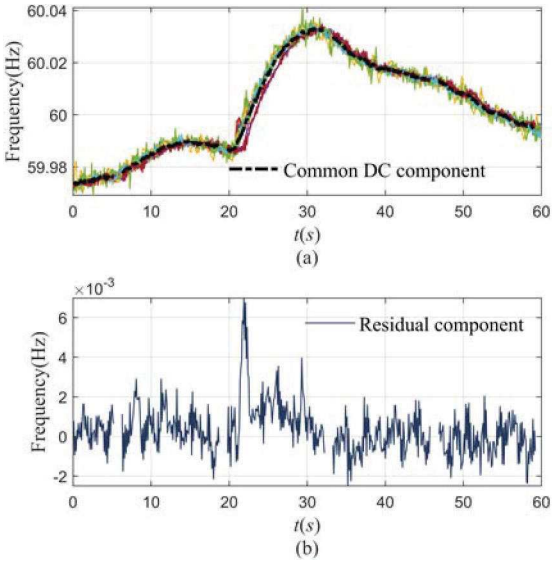

Fig. 2. (a) The measurement frequency and its DC component, (b) the residual component of $x(n)$.

Empirical Mode Decomposition (EEMD) [16]. The time domain modal components of each frequency can be accurately extracted. However, the separated modal signals require further processing to obtain their frequency or statistical domain information.

To this end, the STFT is used, where its advantage is to extract both time and frequency domain information for non-stationary signals.

The definitions of STFT can be denoted as

$$D_n\left(e^{j\omega_k}\right) = \sum_m d(m)\omega(n-m)e^{-j\omega_k m} \tag{1}$$

where $\omega_k = 2\pi k/N$, and k and N are frequency band and the number of frequency bands, respectively. The $\omega(m)$ is the window function with length L.

To be precise, the above equation is also equivalent to

$$D_n\left(e^{j\omega_k}\right) = e^{-j\omega_k n}\bar{D}_n\left(\omega_k\right) \tag{2}$$

The equation (2) can be viewed as the lowpass representations of bandpass filter outputs. Once the window function is selected, the frequency resolution is fixed over all the bands.

979-8-3503-1360-4/24/$31.00 ©2024 IEEE
Authorized licensed use limited to: UNIVERSITY OF TENNESSEE LIBRARIES. Downloaded on September 20,2024 at 14:26:03 UTC from IEEE Xplore. Restrictions apply.

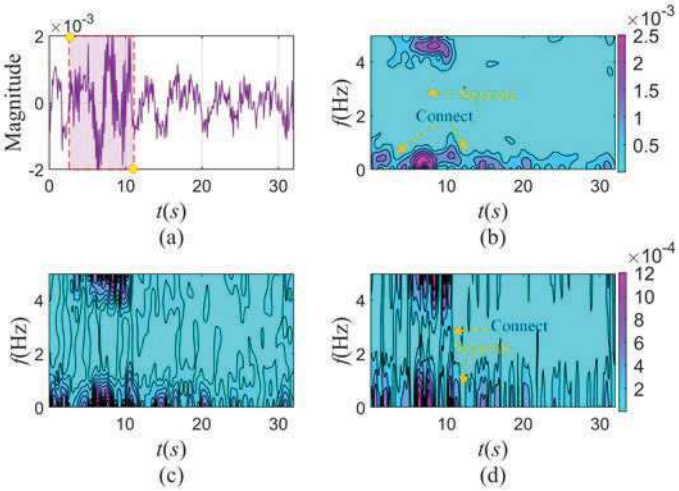

Fig. 3. The STFT of synchrophasor data spoofing attack under different window sizes, where the $\sigma = 0.07$ for all the cases. (a) filter frequency, (b) STFT with $L = 128$, (c) STFT with $L = 64$, (d) STFT with $L = 32$.

In this paper, the symmetric Gaussian window is selected because it is suitable for truncating the non-periodic signals, and it is discrete form can be expressed as

$$\omega(m) = e^{-\frac{1}{2}\left(\frac{m-(L-1)/2}{\sigma(L-1)/2}\right)^2} \tag{3}$$

where σ is the width factor.

To choose a better frequency resolution, a suitable parameter should be determined. In STFT, multiple FFT would be performed to obtain the time-frequency joint distribution. Finally, the magnitude of this D_n can be saved for the next step analysis, which can be denoted as $|D_n\left(e^{j\omega_k}\right)|$.

B. Case analysis for window parameter selection

As mentioned above, the parameters of the window function, including the width factor σ and window size L, would have an impact on the frequency resolution. To investigate the relationship between the measurement synchrophasor data and the parameters, an example of synchrophasor data spoofing attack under different window size L is tested, as shown in Fig. 3. In this case, all the σ is set to 0.07, and the window size L are set to 128, 64, and 32, respectively.

Fig. 3(a) demonstrates that part of the measurement frequency data is intercepted and manipulated by attackers between times 2 to 12 seconds. The manipulated data can easily bypass bad data detection due to its small amplitude change.

Better resolution enables the separation of various components from the time and frequency axes. Compared with Fig. 3(b), (c), and (d), it can be observed that when a larger window size of 128 is used, only some low-frequency and high-frequency components are scattered between 0-1Hz and 4-5Hz. It is possible to distinguish the frequency components more clearly. However, the time-vary between the manipulated and tested signal is still connected. For Fig. 3(c), it has a better time resolution because the manipulated and tested signal can be separated. For Fig. 3(d), it has the best time resolution when L=32 because the energy of the signal is more concentrated. However, the frequency component is connected. This phenomenon is caused by Heinsberg's uncertainty principle.

Based on the above analysis, the L is set to 64 as a trade-off between the time and frequency domain. Next, the spoofing attack would be identified based on $|D_n\left(e^{j\omega_k}\right)|$.

IV. Spoofing Attack Identification Based on YOLO3

After obtaining the $|D_n\left(e^{j\omega_k}\right)|$, the YOLOv3 is introduced to identify the category and time duration of the spoofing attacks.

Modern real-time object detection technology, known as YOLOv3, was developed from the YOLO system [17]. It can detect a 320×320 figure in only 22ms, which is fast enough for the majority of applications. In the grid edge detection, a PMU with a reporting rate of 10Hz would take 100ms to calculate each synchrophasor. Furthermore, the sample can be detected with a step size, this means that YOLOv3 would not slow down the data processing.

The basic structure of YOLOv3 is illustrated in Fig. 1. As with the general convolutional neural networks, the bottom layers of YOLOv3 are two basic units, including the convolutional layer and the pooling layer. The convolutional layer is responded for fingerprint extraction, and the pooling layer is used to filter the redundant features. Additionally, the residual network, sometimes known as the "Res Unit," is designed to expedite training and avoid gradient explosion.

According to Fig. 1, the data set $|D_n\left(e^{j\omega_k}\right)|$, C_d, $[h, l]$ would first pass some residual networks to learn the sufficient fingerprint from measurements, where the $C_d = 0, 1$ denotes that category label and the $[h, l]$ denotes the localization of the spoofing attack. It is worth mentioning that the localization information is mainly transformed by coordinates.

Then, three different scales of boxes Y1, Y2, and Y3 are designed to match the targets of different sizes. The YOLOv3 achieves localization detection by using a bounding box. YOLOv3 may continually enlarge the bounding box until it has the lowest loss by learning the bounding box's coordinate location. Finally, the last of these predict a 3-d tensor encoding bounding box, class predictions.

To train the YOLOv3, the time duration of the spoofing attack would be encoded as coordinates. The yellow circle shown in Fig. 3(a) is an example. The coordinates of the upper left and lower right corners will be marked as a label.

To evaluate the predicted results, the mean average precision (mAP) and F1 score are selected. The mAP is derived from the average precision. Both the larger mAP and F1 values, which means that a better result is obtained.

V. Experiments

To verify the effectiveness of the proposed STFT-based spectrum and Yolo3 model, the synchrophasor frequency collected by 12 Frequency Disturbance Recorders (FDRs) is used. All the devices are distributed in the Western Electricity Coordinating Council system and will be transferred to the FNET/GridEye server located at the University of Tennessee, Knoxville. Each FDR reports data at a rate of 10Hz/s, and the length of each sample is 320.

979-8-3503-1360-4/24/$31.00 ©2024 IEEE
Authorized licensed use limited to: UNIVERSITY OF TENNESSEE LIBRARIES. Downloaded on September 20,2024 at 14:26:03 UTC from IEEE Xplore. Restrictions apply.

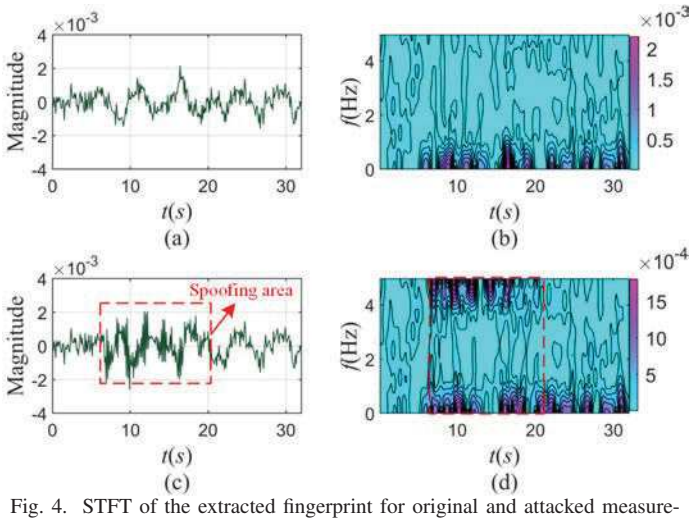

Fig. 4. STFT of the extracted fingerprint for original and attacked measurements. (a) and (c) are the original measurements and attacked measurements, respectively. (b) and (d) are their STFT, respectively.

Only the data from 11 FDRs are utilized for training to replicate the spoofing attack, and one FDR is set aside for data tampering. A total of 18450 samples are created, of which 70% are utilized for training, 15% are used for verification, and the remaining 15% are used for testing. Two categories are used, including the measurement data and the attacked data.

A. Results of extracted fingerprint

To demonstrate the time-frequency fingerprint of the STFT approach, Fig. 4 presents an example of a 32-seconds measured frequency. From Fig. 4(a) and (c) it is observed that the original measurements show consistent time-frequency characteristics.

From Fig. 4(b) and (d) it is found that compared with the original measurements, the time-frequency fingerprint without cyberattacks shows a higher agreement with Fig. 4(c). In contrast, the fingerprint of the spoofing area has a completely different distribution, especially in the high-frequency part where $f = 4Hz$, indicating that STFT can extract the unique fingerprint for synchrophasor data.

Besides, to increase the complexity of the attacks, the compound spoofing attack is also generated. There are two pieces of data were tampered with FDR and simulated event data, as demonstrated in Fig. 5. The first piece of data is attacked by the reserved FDR and the other is tamped with a low-frequency oscillation. It can be seen from Fig. 5 that, the time-frequency information of the spoofing area is different from the original measurements, indicating the effectiveness of the STFT.

If the attacker keeps the measurements (e.g. truly forced oscillation) that occurred before and replaces to with the same PMU, multiple PMU signals can be combined to defend this type of spoofing.

B. Training loss for the YOLOv3

The training loss of the YOLOv3 is depicted in Fig. 6. It reveals that the model is convergent after nearly 60 epochs. Besides, the curves of the training loss and verification loss

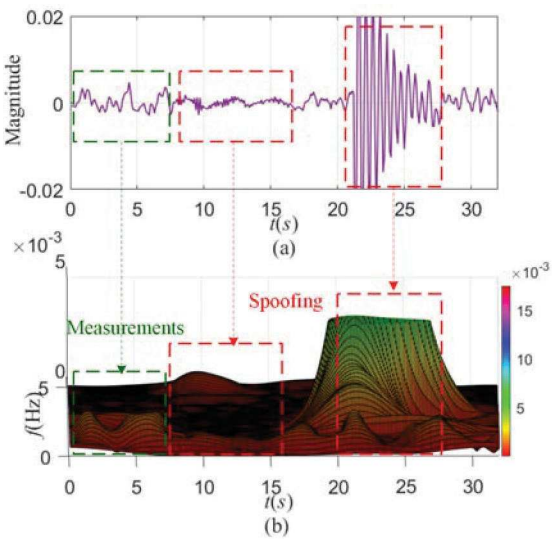

Fig. 5. Example of the compound spoofing attack. (a)measurements with compound spoofing attack, (b) the STFT of (a).

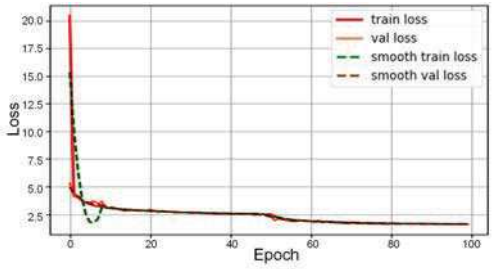

Fig. 6. Training and verification losses of YOLOv3.

are almost overlapped each other, indicating the YOLOv3 is not over-fitting.

C. Performance comparison with different methods

To evaluate the performance of the proposed data security defense framework, two different time-frequency analysis methods are compared, including the Stockwell transform (ST) and Continuous Wavelet Transform (CWT). Besides, the Artificial Neural Network (ANN) is also selected to compare with YOLOv3. The tested results are listed in Table I. Besides, the Yolov5 [18] is also tested combined with STFT.

Compared with ST-YOLOv3, CWT-YOLOv3, and proposed STFT-YOLOv3, it demonstrated that both the mAP and F1 of ST are lower. The F1 and accuracy of CWT are slightly lower than the proposed STFT-YOLOv3. The main explanation could be that the fingerprint feature extraction is affected by the wavelet basis functions. However, the mAP of the CWT is 0.009 higher than STFT. This means that the resolution of STFT can be further optimized. Compared with STFT-ANN, it obtains an accuracy lower than 90%. The primary reason is that YOLOv3 has a stronger learning ability than ANN does. Compared with STFT-YOLOv5, the performance is slightly higher than the proposed method. However, it would consume more time due to its high frames per second [18]. Overall, the STFT-YOLOv3 can be a better choice as a compromise of accuracy and efficiency.

979-8-3503-1360-4/24/$31.00 ©2024 IEEE
Authorized licensed use limited to: UNIVERSITY OF TENNESSEE LIBRARIES. Downloaded on September 20,2024 at 14:26:03 UTC from IEEE Xplore. Restrictions apply.

TABLE I
PERFORMANCE COMPARISON FOR TIME-FREQUENCY METHODS.

Methods	mAP	F1	Accuracy(%)
ST-YOLOv3	0.788	0.85	92.70
CWT-YOLOv3	0.835	0.86	93.58
STFT-ANN	-	0.83	82.25
STFT-YOLOv5	0.842	0.91	94.97
Proposed STFT-YOLOv3	0.826	0.89	94.35

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

Methods	F1	Accuracy(%)	mAP	Localization ability
WT-FFT-ANN [19]	0.88	85.32	-	no
MM-gcForest [15]	0.82	82.57	-	no
EEMD-FFT-BP [6]	0.74	73.68	-	no
FST-MCNN [20]	0.87	91.46	-	no
CWT-CNN [14]	-	84.44	-	no
Proposed STFT-YOLOv3	0.89	94.35	0.826	yes

D. Comparison with some state-of-art methods

The last experiment is to compare with some state-of-art spoofing attack detection methods, including the WT-FFT-ANN [19], MM-gcForest [15], EEMD-FFT-BP [6], FST-MCNN [20], and CWT-CNN [14]. For WT-FFT-ANN and EEMD-FFT-BP, only the frequency information is fed into the spoofing attack framework.

As can be seen from Table II, the WT-FFT-ANN and MM-gcForest get an accuracy in the range of 82% to 86%. The minimal amount of information that was retrieved might be the cause. The CWT-CNN reaches an accuracy higher than 84%, where its advantage is that it can achieve real-time detection for each sample in 1.8ms [14]. For the FST-MCNN, an accuracy higher than 90% is obtained because the MCNN has better learning ability compared with the traditional identification methods.

However, in terms of the spoofing attack localization ability, none of the state-of-the-art techniques mentioned above can pinpoint where or when the spoofing attack occurred due to structural limitations. The detection method can not identify the target without the localization data for training. Based on the aforementioned analysis, the proposed STFT-YOLOv3 has a remarkable performance because it has high-quality input time-frequency information and the ability to locate the spoofing attack.

VI. CONCLUSION

In this paper, a data spoofing attack detection framework named STFT-YOLOv3 is proposed for grid edge data security protection. The time-frequency domain information is extracted as the fingerprint for each device. The visual analysis results of the window parameter selection reveal that the STFT can distinguish the difference between the measurement synchrophasors and the spoofing attack area. Then, the YOLOv3 is designed for the time duration and category detection of the spoofing attack. The experiments demonstrate that the YOLOv3 can accurately and successfully detect single and even compound spoofing attacks with 0.89 mAP and 94.35% accuracy. Importantly, it is possible to discover the time duration of spoofing attacks, which can assist us in figuring out when the data might be utilized again. Our ongoing effort will concentrate on validating the decentralized method to facilitate extension to additional grid edges with alternative data sources.

REFERENCES

[1] G. Wu and Z. Li, "Cyberphysical power system (cpps) A review on measures and optimization methods of system resilience," *Frontiers of Engineering Management.*, vol. 8, p. 503–518, 2021.

[2] H. M. Mustafa and et al., "Cyberpower cosimulation for endtoend synchrophasor network analysis and applications," in *2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2021, pp. 164–169.

[3] M. Ravinder and et al., "A review on cyber security and anomaly detection perspectives of smart grid," in *2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 2023, pp. 692–697.

[4] Wikipedia, "Colonial pipeline ransomware attack, [online] available at:," *https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack*, 2023.

[5] Y. Cui and et al., "Multifractal characterization of distribution synchrophasors for cybersecurity defense of smart grids," *IEEE Transactions on Smart Grid*, vol. 13, no. 2, pp. 1658–1661, 2022.

[6] S. Liu and et al., "Modelfree data authentication for cyber security in power systems," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 4565–4568, 2020.

[7] Y. Zhao and et al., "Passivitybased robust control against quantified false data injection attacks in cyber-physical systems," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 8, pp. 1440–1450, 2021.

[8] R. Meira-Góes and et al., "Towards resilient supervisors against sensor deception attacks," in *2019 IEEE 58th Conference on Decision and Control (CDC)*, 2019, pp. 5144–5149.

[9] Q. He and et al., "A moving target defense strategy against fdia based on flexible switching of spare lines," in *2022 IEEE IAS Industrial and Commercial Power System Asia (ICPS Asia)*, 2022, pp. 1082–1087.

[10] M. Kamal and et al., "Cyberattacks against event-based analysis in micro-pmus: Attack models and counter measures," *IEEE Transactions on Smart Grid*, vol. 12, no. 2, pp. 1577–1588, 2021.

[11] Y. Li and et al., "Detection of false data injection attacks in smart grid: A secure federated deep learning approach," *IEEE Transactions on Smart Grid*, vol. 13, no. 6, pp. 4862–4872, 2022.

[12] Y. Zhang and et al., "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 623–634, 2021.

[13] Y. Cui and et al., "Multiscale adaptive multifractal detrended fluctuation analysis-based source identification of synchrophasor data," *IEEE Transactions on Smart Grid*, vol. 13, no. 6, pp. 4957–4960, 2022.

[14] Q. He and et al., "Machine learning-based cybersecurity defence of wide-area monitoring systems," in *2022 IEEEIAS Industrial and Commercial Power System Asia (I&CPS Asia)*, 2022, pp. 991–996.

[15] Y. Cui and et al., "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.

[16] Z. Li and et al., "Wind power prediction based on eemdtentssalssvm," *Energy Reports*, vol. 8, pp. 3234–3243, 2022.

[17] J. Redmon and A. Farhadi, "Yolov3: An incremental improvement," *arXiv preprint arXiv:1804.02767*, 2018.

[18] U. Nepal and H. Eslamiat, "Comparing yolov3, yolov4 and yolov5 for autonomous landing spot detection in faulty uavs," *Sensors*, vol. 22, no. 2, 2022.

[19] W. Yao and et al., "Source location identification of distribution-level electric network frequency signals at multiple geographic scales," *IEEE Access*, vol. 5, pp. 11 166–11 175, 2017.

[20] W. Qiu and et al., "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.

979-8-3503-1360-4/24/$31.00 ©2024 IEEE
Authorized licensed use limited to: UNIVERSITY OF TENNESSEE LIBRARIES. Downloaded on September 20,2024 at 14:26:03 UTC from IEEE Xplore. Restrictions apply.