Cybersecurity Defence of Synchrophasors in Distribution Systems: A Deep Learning Approach

2023 IEEE International Conference on Energy Technologies for Future Grids
Wollongong, Australia, December 3-6, 2023

Cybersecurity Defence of Synchrophasors in Distribution Systems: A Deep Learning Approach

Ge Zhang[1], Yi Cui [1,2], Ruiyuan Zhang[3] and Feifei Bai [1,4]
[1] School of Information Technology and Electrical Engineering, University of Queensland, Brisbane, Australia
[2]School of Engineering, University of Southern Queensland, Springfield, Australia
[3]Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, China
[4]School of Engineering and Built Environment, Griffith University, Gold Coast, Australia
ge.zhang@uq.edu.au, Yi.Cui@usq.edu.au, zry@ust.hk, f.bai@griffith.edu.au

***Abstract*- Phasor Measurement Unit (PMU) has become a critical component for the modern distribution network, as it records high-resolution synchrophasor data which contain abundant static and dynamic information of the system. However, PMUs are vulnerable to potential cyberattacks, for example, data spoofing attacks. A deliberate PMU spoofing attack can confuse the existing data source authentication models, especially when the models are used for identifying multiple PMUs at the same time. This paper proposes a data-driven cybersecurity defence model which can identify the source information of a large group of PMUs with high accuracy. The model utilizes the inherent correlations among PMUs with a deep neural network to enhance the data source authentication performance. The effectiveness of the proposed model is examined by the PMU data collected from a real distribution network with different error metrics. Through comprehensive numerical experiments, the proposed model provides consistent superior performance in comparison with other state-of-the-art data source identification approaches.**

Keywords-Source identification, deep learning, cybersecurity, distribution system, PMU.

NOMENCLATURE

F	Frequency Series Data
FP	False Positive
FN	False Negative
RFRM	Regional Frequency Residual Matrix
RVRM	Regional Voltage Residual Matrix
TP	True Positive
TN	True Negative
V	Voltage Series Data

I. INTRODUCTION

The distribution system is a complex network which contains tremendous nodes, branches, switches, etc. With the increasing integration of renewable energy sources into the system, traditional passive consumers have been transforming into active prosumers. It is critical to monitor and control the distribution system in a real-time manner [1]. Therefore, modern distribution systems have equipped with many advanced metering devices like PMUs. The wide usage of smart devices and advanced information and communication technologies in the last decades are also promoting monitoring systems' dynamic behaviours using their measurements [2].

Though advanced devices such as PMUs are used to improve grid efficiency and reliability, these devices are facing many security issues, especially cybersecurity [3]. For instance, the absence of cybersecurity mechanisms in the commonly employed PMU data frame has raised significant concerns about the PMU's resilience against potential data integrity attacks [4]. Ensuring the stability and reliability of the smart grid in the future has become a paramount priority. Hence, it becomes crucial to devise cybersecurity defence schemes that exhibit both high reliability and efficiency in order to authenticate the source locations of PMU data stored in the server.

Over the past several years, great efforts have been put forward to develop PMU data source authentication strategies which can be categorized into two groups: physical model-based and data-driven approaches. For the physical model-based approaches, Ref [5] proposed a novel Jaccard dissimilarity index-based method to achieve an accurate identification of tripped branches subjected to data integrity attacks. Further, a distributed state estimator with an event-triggered detection against data integrity attacks in wireless sensor networks was developed in [6]. In [7], an online chi-square detection method was proposed by using a particle swarm optimization algorithm. To overcome the limitation of physical-model-based approaches in terms of the requirement of complete network topology and accurate parameters, several data-driven approaches have been developed to authenticate the source information of PMU measurements, including support vector machine [8], random forest [9], artificial neural networks [10-11], convolutional neural networks [12-13], et al. These data-driven methods generally exploit the spatial and temporal signatures from PMU measurements and then use the extracted signatures to train the machine learning algorithms so that the spatiotemporal signatures and associated source locations of PMUs are correlated. The well-trained machine learning algorithms will be further used to authenticate (classify) the source information of new PMU data of interest.

Currently, most data source authentication studies only have been designed and tested on a relatively small PMU dataset. The geographic distribution of the PMUs in previous studies is dispersed at a large geographical scale as well, such as inter-state level [10-12]. The performance of existing methods on near PMUs has not been carefully evaluated yet. Therefore, this paper proposes a data-driven approach to achieve accurate source authentication on the PMU measurements collected from the real distribution network. In contrast to prior research, the

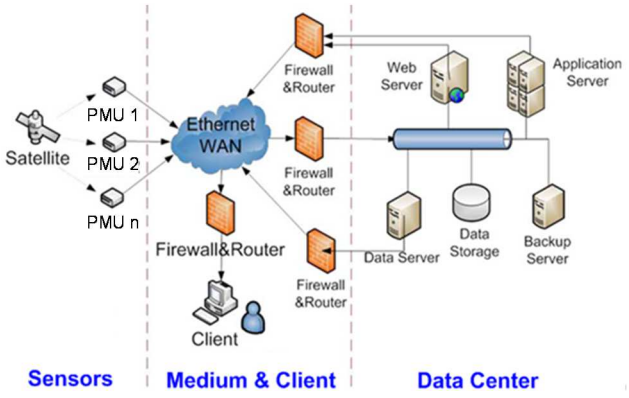
978-1-6654-7164-0/23/$31.00

presented work showcases a notably larger number of PMUs (33 PMUs) while focusing on a relatively smaller geographic scale (i.e., intra-state locations of multiple 11kV feeders within a power network in Queensland state). Comprehensive experiments on the performance of different data source authentication models are conducted. The experiments have shown that the proposed model can provide robust and effective authentication accuracy compared to other baseline methods.

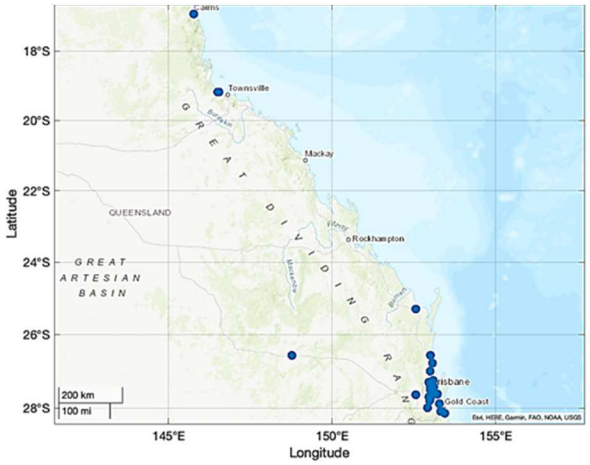
The main contributions of this paper can be summarized as follows: (1) The inception of a universal power system network security monitoring methodology, 'FDNET', grounded in regional PMU data has been proposed. (2) The proposed method has demonstrated marked advancement over contemporaneous state-of-the-art approaches with respect to classification problems involving a large number of PMUs. (3) The considerable practical implications and the inherent value of the presented model are further reinforced through the application of operational data obtained from extant power networks.

II. Proposed Deep Learning-Based Source Authentication Method

As a system-wide critical parameter of the power system, frequency reflects the balance between energy generation and consumption. Previous studies have shown that intrinsic temporal characteristics contained in the frequency signal can be used for authenticating data sources [9]. It is because the frequency measured within close interconnections shares a similar trend due to the synchronicity of a power system. In the distribution network, the load difference between upstream and downstream will cause relatively constant small deviations in the frequencies, which can be precisely measured by PMUs. This measured bias can be used as an important feature to identify specific PMUs. Moreover, the spatial correlation among PMUs data has also been applied to detect the spoofing attack on PMUs. As shown in Fig. 1, a PMU-based condition monitoring system consists of a large number of PMUs at multiple measurement locations and then collects and transfers the frequency data in less than 30 milliseconds from all locations to a data server using standard communication protocols. This paper uses PMU data from 33 locations within a distribution network of eastern Queensland as shown in Fig 1(b).



(a)



(b)

Fig. 1 (a) Hardware connection of a PMU-based monitoring system and (b) locations of PMUs within a distribution network

A. Data Pre-processing

To ensure high data quality, anomaly detection and removal are conducted when constructing the original frequency-based categorical features. In this work, the frequency bias which is greater than 0.1Hz is regarded as an abnormal data point. After the outlier detection and removal, the frequency sequence will be smoothed by a moving average interpolation algorithm based on adjacent information to maintain the original data dimension. Data points with amplitudes between 0.998pu and 1.002pu will be preserved to construct categorical features.

B. Normalization

a) Zero-mean normalization

In order to establish a standardized feature dataset and improve the training performance of the model, a data normalization process is necessary. Zero-mean normalization and Zero-score standardization are commonly used.

Given a segment $X = \{x_0, x_1, x_2, \dots \dots, x_n\}$ in a standard sampling window, the process of Zero-mean normalization can be written as (1).

$$x_n' = \frac{(x_n - x_{mean})}{(x_{max} - x_{min})} \tag{1}$$

Zero-mean normalization is a linear transformation of the original data, and the result will be mapped between 0 and 1. It is worth noting that the new input data may lead to some changes in x_{max} and x_{min}, so that the normalization standard may need to be redefined simultaneously.

b) Zero-score normalization

The Zero-score normalization can be expressed as (2).

$$x_n' = \frac{X_n - X_{mean}}{Standard\ deviation} \tag{2}$$

Through Zero-score normalization, the processed data will conform to a standard normal distribution. The mean value of the processed data will be zero and the standard deviation will be one. This characteristic may change the relative magnitude of some hazards.

C. Regional Frequency Residual Matrix (RFRM)

In order to achieve accurate identification of multiple PMUs, in addition to the features of a local PMU, the regional difference also needs to be considered. In this paper, we use the outlier-cleaned frequency data of the PMUs to build the RFRM as the classification feature.

Assuming that data from n PMUs are collected and the length of the sampling time window is I, then the frequency of the target PMU_0 in the time window can be noted as $F_0 = f_0^1, f_0^2, f_0^3, \dots, f_0^I$. In order to reflect the frequency difference between PMUs in RFRM, each row of the matrix represents the frequency residuals of the target PMU_0 and the rest each PMU_n. In this way, for each time window of PMU_0, a regional frequency residual feature matrix of size $a \times b$ $(a = n-1, b = i)$ will be generated. The value of RFRM elements can be determined by $r_{ab} = f_0^i - f_n^i \; where \; i = 1,2,3,\dots,I \; and \; n = 2,3,\dots,N$. The constructed RFRM can be written as (3a).

$$[RFRM] = \begin{bmatrix} F_0 - F_1 \\ F_0 - F_2 \\ F_0 - F_3 \\ \vdots \\ F_0 - F_{n-1} \end{bmatrix} = \begin{bmatrix} f_1^1 & f_1^2 & f_1^3 & \cdots & f_1^{i-2} & f_1^{i-1} & f_1^i \\ f_2^1 & f_2^2 & f_2^3 & \cdots & f_2^{i-2} & f_2^{i-1} & f_2^i \\ f_3^1 & f_3^2 & f_3^3 & \cdots & f_3^{i-2} & f_3^{i-1} & f_3^i \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ f_{n-1}^1 & f_{n-1}^2 & f_{n-1}^3 & \cdots & f_{n-1}^{i-2} & f_{n-1}^{i-1} & f_{n-1}^i \end{bmatrix} \quad (3a)$$

Since existing literature also used phase voltage for PMU data source authentication, this paper also builds the regional voltage residual matrix, RVRM, by following the same steps to build RFRM as (3b). RFRM and RVRM will be used as the feature input of the classifier in the following section for comparison purposes.

$$[RVRM] = \begin{bmatrix} V_0 - V_1 \\ V_0 - V_2 \\ V_0 - V_3 \\ \vdots \\ V_0 - V_{n-1} \end{bmatrix} = \begin{bmatrix} v_1^1 & v_1^2 & v_1^3 & \cdots & v_1^{i-2} & v_1^{i-1} & v_1^i \\ v_2^1 & v_2^2 & v_2^3 & \cdots & v_2^{i-2} & v_2^{i-1} & v_2^i \\ v_3^1 & v_3^2 & v_3^3 & \cdots & v_3^{i-2} & v_3^{i-1} & v_3^i \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ v_{n-1}^1 & v_{n-1}^2 & v_{n-1}^3 & \cdots & v_{n-1}^{i-2} & v_{n-1}^{i-1} & v_{n-1}^i \end{bmatrix} \quad (3b)$$

D. FDNET

Existing studies in the area of deep learning showed that a deeper network allows better feature extraction capabilities [12-13]. However, when the network depth reaches a certain level, just continuing to stack more layers to the model will cause many drawbacks. Firstly, the gradients may vanish or explode which will have a negative impact on reducing the loss. This trouble can be solved by adding layers or introducing better network initialization. The second problem is degradation. When the number of network layers is saturated, continuing to add layers will cause difficulties in optimization, so the training error and prediction error will become larger. It is worth noting that the error growth here is not caused by over-fitting. Therefore, the traditional parameter tuning method for overfitting will no longer apply.

Two improvements need to be done to solve the problem of degradation. The first one is to add residual information to the mainstream. The intensive training of the model is carried out by using the differential features represented by the residuals, which not only improves the training efficiency but also makes the model pay more attention to discovering and learning the differences between the input information. The second improvement is crossline chaining. This additional chain can be analogous to the principle of proportional-integral controller widely used in control engineering, one branch focuses on processing the differentiated information of categorical features, and the other branch retains the original features and adds the residual information at the confluence point. In this way, the output information at the exit of the module can not only retain the original information but also represent a certain change at the same time. With this mechanism, ResNet can solve the thorny convergence problem of complex models.

The proposed model contains three basic structures, UNIT1, UNIT2 and UNIT3, all of which follow the principle of crossline chaining. UNIT1 and UNIT2 have the same structure for the residual information flow branch, and both consist of three convolutional layers and two Rule function layers as shown in Fig 2. UNIT3 changes the first layer from Relu to Max-pool. Another difference between them is that the original information flow branch of UNIT1 does not perform any processing and completely retains the original information. UNIT2 and UNIT3 perform convolution on the original information after the Relu layer and then feed it forward to the Add and Norm layer at the output of the module. The proposed FDNET contains all three basic structures mentioned above. The specific structural framework is shown in Fig 3.

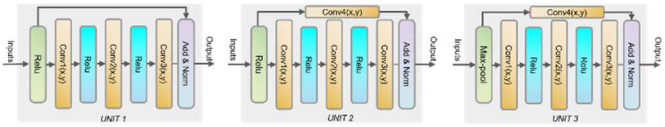


Fig. 2 . *UNIT structures*

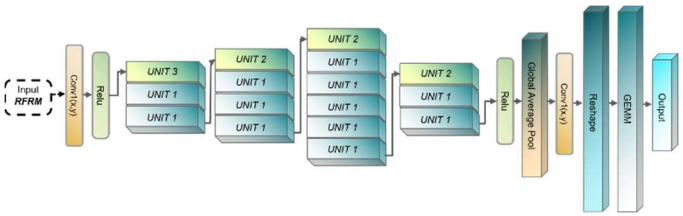


Fig. 3. *Basic structure of the proposed FDNET*

III. CASE STUDIES AND RESULTS DISCUSSION

A. Experiment Setup

The proposed PMU data source authentication method is verified by conducting experiments on a PMU dataset, which comprises three months of data from 33 intra-state locations within a distribution network in Queensland. The PMU data has a sampling time of 20ms. To construct the experimental dataset, 1000 segments, each consisting of 20-second synchrophasor measurements, are utilized for each location. For the FDNET training, 80% of the segments are randomly selected, while the remaining 20% are reserved for testing purposes. The algorithm's performance is evaluated by classification accuracy, precision, recall, F-1 score as well as the time required to authenticate each testing sample.

The classification accuracy is defined as (4).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (4)$$

where TP means true positive, which indicates the positive samples that are predicted to be positive. FP means false positive, which represents the negative samples that are predicted to be positive. Similarly, TN and FN represent the negative samples that are predicted to be negative and the positive samples that are predicted to be negative respectively. Considering the data can be extremely biased when the attacks occur, using accuracy alone is not enough to fully evaluate the pros and cons of a method. Therefore, more indicators need to be used.

Precision is defined as the probability of a sample that is actually positive among all samples that are predicted to be positive as (5). This can be seen as the prediction accuracy of positive samples.

$$Precision = \frac{TP}{TP + FP} \quad (5)$$

Moreover, recall is defined as the probability of being predicted as a positive sample among the samples that are actually positive as (6).

$$Recall = \frac{TP}{TP + FN} \quad (6)$$

The F1-score can be seen as an average of model precision and recall. It is an indicator used in statistics to measure the accuracy of the binary classification model. Thanks to the fact that the F1-score takes into account both the precision and recall of the classifier, compared to accuracy, F1-score can evaluate the performance of the model more completely.

$$F_1 = 2 \times \frac{percision \times recall}{percision + recall} \quad (7)$$

1) Comparison of frequency feature and voltage feature

Compared with the local frequency collected by PMU, the voltage will fluctuate in a larger range for a practical network. Taking Australia as an example, the frequency is concentrated around 50Hz. Considering the 5% active power droop coefficient that is commonly used by synchronous generators in the power grid, the maximum frequency fluctuation caused by output control under normal operating conditions is 0.25Hz. Under normal circumstances, the frequency adjustment in the full power range is rarely achieved, so the frequency fluctuation caused by the output adjustment of a single power node in a steady state is often much smaller than the above value.

Assuming that one generator uses 50% of the active power reserve to participate in frequency regulation, this will keep the local frequency in a very narrow range of 49.875Hz to 50.125Hz, which reflects an obvious global normalized steady-state characteristic of the grid frequency. But the voltage does not have this characteristic. The difference in voltage levels is one of the main reasons, which makes the large variation in voltage magnitude. Secondly, the differences in the load characteristics and the tap changer will also lead to large irregular fluctuations in the steady-state voltage. These fluctuations make the outliers in voltages more difficult to monitor and define and thus influence the accuracy and efficiency of data pre-processing. Similar conclusions are also reflected in the training and validation process. In this paper, the single frequency feature and single voltage feature of 33 PMUs are used for comparative experiments, and outlier detection and moving average interpolation are performed on both data.

According to Fig. 4, the FDNET proposed in this paper can achieve high classification accuracy both on the RFRM and RVRM datasets. The training accuracy by using RVRM is about 5% higher than that using RFRM features. However, the fluctuation of the validation accuracy with the RVRM feature is much larger than the frequency feature. The standard deviation of validation accuracy of RVRM is 13.6 % which is much larger than 3.4% with RFRM. In other words, using RVRM may lead to overfitting more easily than RFRM. When using RFRM, the verification accuracy can follow the training accuracy better, which reflects stronger robustness and higher practical application value.

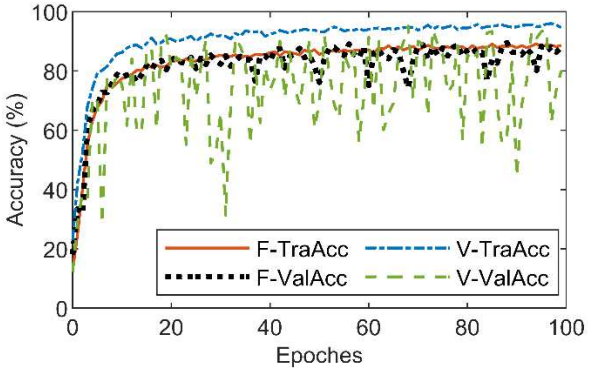
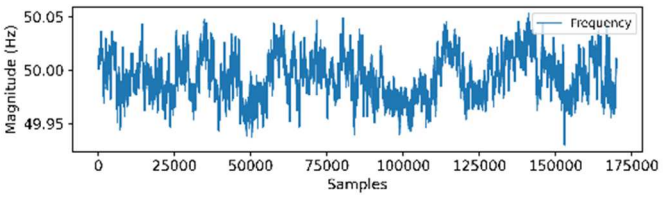


Fig. 4. Accuracy comparison by using RFRM and RVRM

2) Comparison of different normalization methods

The pre-process of normalization can rescale the original data, especially the phase voltage data, into a unified range. Normalized input can provide the potential scalable ability to the classifier. The importance of this scalable ability will be more significant when the classifier is deployed to a bulk system with a large geographical area and multi-topology levels. Therefore, to ensure the performance of the classifier, a proper normalization method needs to be well selected and turned. A sample set of frequency and voltage measurements is shown in Fig. 5. The mathematical differences between Zero-means and Zero-score normalization have already been discussed in the previous Section II.B. According to Fig. 6, the standard deviation of validation accuracy by using Zero-mean normalization is 3.3% less than using Zero-score normalization. In other words, using RFRM and Zero-Mean normalization together has better robustness than the other conditions.



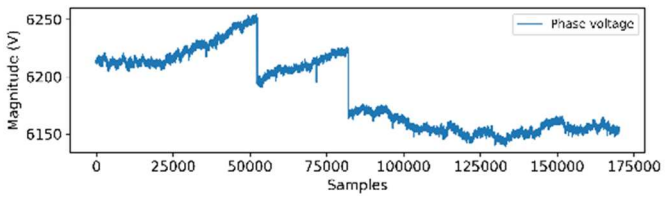


Fig. 5 Original input frequency and phase voltage data from PMUs

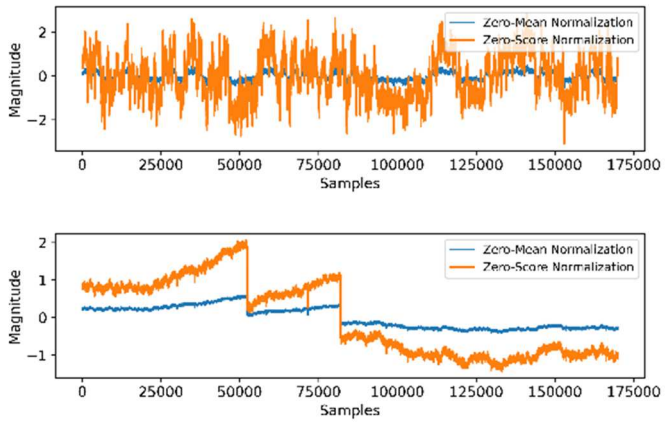


Fig. 6. Frequency and phase voltage data normalized by zero-mean and zero-score methods

B. Results Discussion

To demonstrate the performance of the proposed deep learning-based source identification method, four "state-of-the-art" source authentication approaches (including both traditional shallow learning-based methods and advanced deep learning-based methods) are selected for comparison purposes which are described in Table I. The source authentication results are summarized in Table II.

TABLE I COMPARISON OF DIFFERENT SOURCE AUTHENTICATION METHODS

Reference	No. of PMUs	Feature domain	Methods	PMU data source used in literature
[10]	3	T&F	EEMD -FFT-BP	FNET/GridEye, Knoxville, TN, USA
[11]	15	T&F	WT-ANN	FNET/Grideye, (Missouri, Tennessee, South Carolina, West Virginia, and Florida), USA
[12]	10	T&F	CWT-CNN	Western Interconnection (WECC) system, USA
[13]	3	T	1D-CNN-GRU	FNET/GridEye Knoxville, TN, USA
Proposed	33	T	FDNET	Eastern Network, Queensland, Australia

*T: time domain, F: frequency domain

TABLE II PERFORMANCE COMPARISON OF DIFFERENT SOURCE AUTHENTICATION METHODS

Data	Metrics		Methods				
			[13]	[10]	[11]	[12]	Proposed
33 PMU	ACC	Training	0.96	0.52	0.58	0.93	0.93
		Testing	0.86	0.45	0.57	0.85	0.92
	Precision		0.86	0.45	0.57	0.85	0.9
	Recall		0.86	0.45	0.57	0.85	0.88
	F1-score		0.86	0.45	0.57	0.85	0.89
Authentication time per sample			>2s	250ms	<1ms	11ms	4.5ms

Compared with other methods in a similar field, ensemble empirical mode decomposition (EEMD) is used in [10] to decompose the original data into several intrinsic mode functions (IMFs) and the residual, then the fast Fourier transform (FFT) is further employed to obtain the characteristics in the frequency domain, which are utilized as the input data of a neural network. This solution can achieve 52% training accuracy and 45% testing accuracy on the 33 PMU dataset. However, in this method, the source authentication takes a longer time (i.e., 250ms) to complete since EEMD and FFT are the loops that heavily depend on computing resources, so the performance of this method on large-scale PMU classification tasks is not ideal.

Another source authentication method that combines a wavelet-based signature extraction and feedforward artificial neural network is presented in [11]. Although this method takes the least time to complete the source authentication, it only obtains 58% training accuracy and 57% testing accuracy on the 33 PMU dataset which is slightly better than the method in [10].

For the source authentication method proposed in [12], it first utilizes the continuous wavelet transform (CWT) to decompose PMU data. Then, the dual-frequency scale convolutional neural networks (DSCNN) are proposed to identify the time-frequency matrix from two frequency scales. This method obtained an overall 93% training accuracy and 85% testing accuracy on the 33 PMU dataset and the authentication time is 11ms per testing sample.

Paper [13] utilized a one-dimensional convolutional neural network (1D-CNN) to extract temporal signatures hidden in frequency, voltage angle and amplitude data. After that, the gated recurrent unit (GRU) will employ these temporal signatures for data source authentication. The 1D-CNN-GRU-based method can achieve 96% training accuracy and 86% testing accuracy on the 33 PMU dataset which is comparable to the method of [12]. However, it takes the longest time (i.e. more than 2 seconds) to complete the source authentication which is impractical for real-time applications in the power grids.

Compared with these benchmark methods, the proposed FDNET achieved the highest recognition accuracy in a dataset composed of 33 real-world PMUs. FDNET's accuracy surpasses that of the best-performing benchmark method by approximately 7%, and it also garners an increase of over 5% in performance metrics for evaluating models on asymmetrical datasets, such as precision, recall, and F1-score. These leading metrics amply testify to FDNET's enhanced robustness. Simultaneously, FDNET processes each sample 59% faster than the benchmark model with the highest accuracy, reaching 4.5 milliseconds per sample, thereby conclusively illustrating its efficiency.

Fig. 7 shows the training and testing accuracy and loss of the proposed method using zero-mean and zero-score normalization and RFRM features. It is clear that the deep

learning algorithm achieves the best source authentication performance by using zero-mean normalization. Compared to other counterparts, the proposed deep learning-based source authentication method attains the highest identification accuracy (i.e., 92%). Additionally, the time consumed for each testing sample is 4.5ms as presented in Table II. Considering the sampling rate of the installed PMU is 50Hz, the source authentication can be completed before a new data point is collected. In other words, the real-time application can also be satisfied.

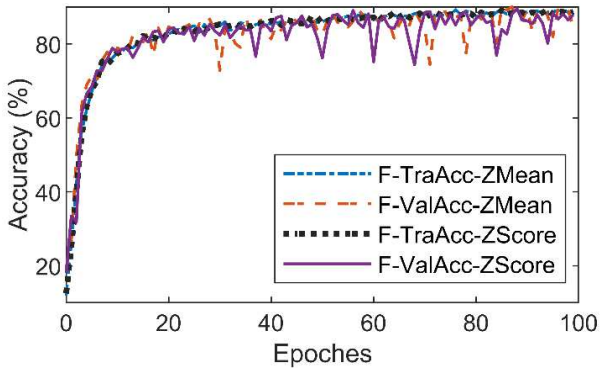


Fig. 7. Accuracy comparison of using Z-Mean and Z-score with RFRM

It is worth noting that the dataset used in the case study contains 15% extremely close PMUs. Since the electrical distance and topological characteristics are almost the same, the frequency data collected by these PMUs are extremely similar, creating difficulty for deep learning algorithms to fully identify the source locations. Of course, it is possible to accurately classify adjacent PMUs by simultaneously collecting multiple channels of information and performing complex time-frequency domain feature extraction, but the surge in data investment and computing power requirements will greatly limit the industrial application of this solution. A feasible solution is to pass the low-reliability data into the cascaded secondary layer after the primary classification layer completes the preliminary task to accurately identify the neighbourhood PMU. If there is no need, the second-level classification layer may not be called. This scheme can not only guarantee the identification speed of PMUs in the wide area network but also ensure classification accuracy under different density conditions. Due to space limitations, this paper will not discuss the above solutions in depth. But this hierarchical idea can be used as a very possible direction for future research.

IV. CONCLUSIONS

To protect the power system's stable operation from various cyber-attacks, this paper proposed a time domain-based cyber threat detection framework. Based on the frequency data collected by the widely installed PMU along the east coast of Queensland, Australia, the RFRM can be first built by using the differential value of the local node and the others. Then, FDNET is proposed to define the RFRM credibility, and the spoofing activity can be clearly identified by validating the credibility of each node. The proposed method has a high potential to be deployed in real power systems which provides network operators with insight into the legitimate variations of power system measurements to avoid data integrity attacks and further improve the security of networks.

Neighbourhood PMU will lead to performance degradation of general-purpose classifiers. At the end of this paper, the possibility of a two-level classification architecture to solve the classification accuracy problem at different densities is discussed. This architecture based on cascade classification is likely to become a key direction of future research in this field.

REFERENCES

[1] NASPI, "Synchronized Measurements and their Applications in Distribution Systems: An Update Draft,", 2020.
[2] K. Gai, K. Xu, Z. Lu, M. Qiu and L. Zhu, "Fusion of Cognitive Wireless Networks and Edge Computing," *IEEE Wireless Commun.*, vol.26, Issue 3, pp. 69-75, 2019.
[3] Y. Cui, F. Bai, Y. Liu, P. Fuhr and M. Morales-Rodriguez, "Spatio-Temporal Characterization of Synchrophasor Data Against Spoofing Attacks in Smart Grids," *IEEE Trans. Smart Grid*, vol.10, Issue 5, pp. 5807-5818, 2019.
[4] R. Khan, K. McLaughlin, D. Laverty and S. Sezer, "IEEE C37.118-2 Synchrophasor Communication Framework: Overview, Cyber Vulnerabilities Analysis and Performance Evaluation," *2nd International Conference on Information Systems Security and Privacy*, 2016, Rome, Italy, pp. 1-10.
[5] M. Alam, S. Kundu, S. Sankar Thakur and S. Banerjee, "A Maiden Application of Jaccard Similarity for Identification of Tripped Branch Utilizing Current Synchronized Measurement Considering False Data Injection Attack," *Measurement*, vol.196, pp. 111259, 2022.
[6] W. Yang, L. Lei and C. Yang, "Event-Based Distributed State Estimation Under Deception Attack," *Neurocomputing*, vol.270, pp. 145-151, 2017.
[7] R. Chen, X. Li, H. Zhong and M. Fei, "A Novel Online Detection Method of Data Injection Attack Against Dynamic State Estimation in Smart Grid," *Neurocomputing*, vol.344, pp. 73-81, 2019.
[8] W. Qiu, Q. Tang, K. Zhu, W. Yao, J. Ma and Y. Liu, "Cyber Spoofing Detection for Grid Distributed Synchrophasor Using Dynamic Dual-Kernel SVM," *IEEE Trans. Smart Grid*, vol.12, Issue 3, pp. 2732-2735, 2021.
[9] Y. Cui, F. Bai, Y. Liu and Y. Liu, "A Measurement Source Authentication Methodology for Power System Cyber Security Enhancement," *IEEE Trans. Smart Grid*, vol.9, Issue 4, pp. 3914-3916, 2018.
[10] 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 Trans. Smart Grid*, vol.11, Issue 5, pp. 4565-4568, 2020.
[11] W. Yao, J. Zhao, M. J. Till, S. You, Y. Liu, Y. Cui and Y. Liu, "Source Location Identification of Distribution-Level Electric Network Frequency Signals at Multiple Geographic Scales," *IEEE Access*, vol.5, pp. 11166-11175, 2017.
[12] W. Qiu, K. Sun, W. Yao, S. You, H. Yin, X. Ma and Y. Liu, "Time-Frequency Based Cyber Security Defense of Wide-Area Control System for Fast Frequency Reserve," *Int. J. Electr. Power Energy Syst.*, vol.132, pp. 107151, 2021.
[13] S. Liu, S. You, C. Zeng, H. Yin, Z. Lin, Y. Dong, W. Qiu, W. Yao and Y. Liu, "Data Source Authentication of Synchrophasor Measurement Devices Based On 1D-Cnn and Gru," *Electr. Power Syst. Res.*, vol.196, pp. 107207, 2021.