Multifractal Characterization of Distribution Synchrophasors for Cybersecurity Defense of Smart Grids

Yi Cui, *Senior Member, IEEE*, Feifei Bai, *Senior Member, IEEE*, Ruifeng Yan, *Member, IEEE*, Tapan Saha, *Fellow, IEEE*, Mehdi Mosadeghy, *Member, IEEE*, Hongzhi Yin, *Member, IEEE*, Ryan K. L. Ko, *Member, IEEE*, and Yilu Liu, *Fellow, IEEE*

***Abstract*—“Source ID Mix” spoofing emerged as a new type of cyber-attack on Distribution Synchrophasors (DS) where adversaries have the capability to swap the source information of DS without changing the measurement values. Accurate detection of such a highly-deceptive attack is a challenging task especially when the spoofing attack happens on short fragments of DS recorded within a relatively small geographical scale. This letter proposes an effective approach to detect this cyber-attack by realizing the multifractal characteristics of DS measurements. First, the multifractal cross-correlation of DS measured at multiple intra-state locations is revealed. Then the derived correlation is integrated with weighted two-dimensional multifractal surface interpolation to reconstruct quasi high-resolution signals. Finally, informative location-specific signatures are extracted from the high-resolution DS and they are integrated with advanced machine learning techniques for source authentication. Experiments using the real-life DS are performed to verify the proposed method.**

***Index Terms*—Source ID Mix, distribution network, cyber-physical security, OT security, phasor measurement unit (PMU).**

I. Introduction

With the high accuracy and resolution measurements of Phasor Measurement Units (PMUs), DS provide system operators with an unprecedented way to achieve real-time monitoring and control of power systems. However, due to the lack of a perfect data authentication mechanism of PMU communication protocol-IEEE C37.118, the data security of DS is always vulnerable to cyber spoofing attacks [1]. Even IEC 61850-90-5 recommends the communication security of the PMU protocol, sophisticated data attacks can still be initiated by potential adversaries. “Source ID Mix” represents a new type of sophisticated data spoofing attack of DS which may threaten critical DS-based monitoring and control, such as inter-area low-frequency oscillation damping control and electromechanical disturbance location estimation [2]. Therefore, reliable detection of this attack provides substantial benefits to system operators for ensuring the data integrity and security of many DS-based applications in smart grids.

To address the cybersecurity challenges raised by sophisticated data spoofing attack, several cybersecurity defense methods have been developed. Depending on the robustness of methods, these approaches can be divided into two major streams, i.e., *model-based* approaches and *model-free* approaches [1]. *Model-based* approaches usually first establish state equations of the power network and then examine the residual vectors or state variables to identify if any abnormal changes occur in the DS measurements. However, the need for system structures and parameters for building the state equations limits its generality and adaptability in detecting spoofing attacks on DS. To overcome the above limitations, *model-free* methods detect the spoofing attack by extracting informative location-specific signatures embedded in the DS and integrating the extracted signatures with machine learning techniques, such as Support Vector Machine (SVM) [3], Artificial Neural Networks (ANN) [4], Random Forest Classification (RFC) [5] and deep learning algorithms (such as Deep Forest - DF [2] and Convolutional Neural Network -CNN [6]–[7]. However, how to accurately extract the above signatures and achieve reliable detection is still challenging.

By nature, the variation of DS has the characteristics of duality in both spatial and temporal domains, i.e., relevance and randomness. Therefore, the identification accuracy of the source locations mainly depends on how much the spatio-temporal signatures of the DS from each local environment differentiate from each other. For DS collected from wide-area locations (e.g., inter-country, interconnection or inter-state), most methods can achieve reasonably high identification accuracy (above 90%). For DS measured from dense locations (i.e., grid within the same state or even within the same city), the

Manuscript received May 22, 2021; revised October 19, 2021; accepted November 25, 2021. Date of publication December 3, 2021; date of current version February 21, 2022. This work was supported in part by the UQ Cyber Transdisciplinary Research Seed Funding; in part by the Queensland State Government, Australia, through the Advance Queensland Research Fellowship under Grant AQIRF0022018; in part by the UQ EAIT Early Career Researcher Philanthropic Grants; in part by the Advance Queensland Platform Technology Program under Grant AQPTP01216-17RD1; and in part by the University of Queensland Solar, Australia (UQ Solar; solar-energy.uq.edu.au). Paper no. PESL-00119-2021. *(Corresponding author: Feifei Bai.)*

Yi Cui, Ruifeng Yan, Tapan Saha, Hongzhi Yin, and Ryan K. L. Ko are with the School of Information Technology and Electrical Engineering, The University of Queensland, Brisbane, QLD 4072, Australia (e-mail: y.cui3@uq.edu.au; ruifeng@itee.uq.edu.au; saha@itee.uq.edu.au; h.yin1@uq.edu.au; ryan.ko@uq.edu.au).

Feifei Bai is with the School of Information Technology and Electrical Engineering, The University of Queensland, Brisbane, QLD 4072, Australia, and also with the School of Engineering and Built Environment, Griffith University (Gold Coast Campus), Southport, QLD 4222, Australia (e-mail: f.bai@uq.edu.au).

Mehdi Mosadeghy is with the Research and Development Department, NOJA Power, Brisbane, QLD 4172, Australia (e-mail: mehdim@nojapower.com.au).

Yilu Liu is with the Department of Electrical Engineering and Computer Science, The University of Tennessee, Knoxville, TN 37996 USA, and also with Oak Ridge National Laboratory, Oak Ridge, TN 37831 USA (e-mail: liu@utk.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSG.2021.3132536.

Digital Object Identifier 10.1109/TSG.2021.3132536

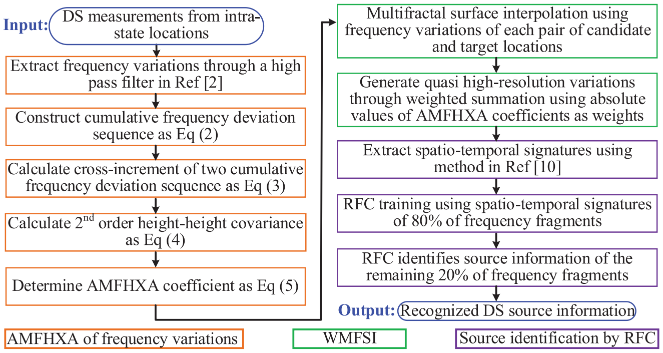
Input:
DS measurements from intra-state locations
Extract frequency variations through a high pass filter in Ref [2]
Construct cumulative frequency deviation sequence as Eq (2)
Calculate cross-increment of two cumulative frequency deviation sequence as Eq (3)
Calculate 2nd order height-height covariance as Eq (4)
Determine AMFHXA coefficient as Eq (5)
Multifractal surface interpolation using frequency variations of each pair of candidate and target locations
Generate quasi high-resolution variations through weighted summation using absolute values of AMFHXA coefficients as weights
Extract spatio-temporal signatures using method in Ref [10]
RFC training using spatio-temporal signatures of 80% of frequency fragments
RFC identifies source information of the remaining 20% of frequency fragments
Output:
Recognized DS source information
AMFHXA of frequency variations
WMFSI
Source identification by RFC

Fig. 1. Proposed cybersecurity defense framework.

identification accuracy is normally less than 90% as variations of the measured DS from these locations exhibit high similarity. Although the identification accuracy can be further improved to above 90%, DS with a high reporting rate and longer time interval (e.g., 120Hz reporting rate and 10 minutes length [5]) are required to realize the spatio-temporal signatures which may not be feasible for protecting real-time DS-based applications (for example, low-frequency disturbance mode identification and localization usually relies on 20 seconds data). Therefore, the main contribution of this letter is to achieve reliable source authentication of short DS fragments from near range (i.e., intra-state) locations without upgrading the hardware of the PMU device. The findings of this paper have the potential to address the cybersecurity challenges raised by the "Source ID Mix" spoofing attack.

II. Proposed Cybersecurity Defense Framework

By examining the multifractality of DS recorded at the individual location, the authors found frequency variations over a large geographical scale (i.e., Eastern Interconnection in the U.S.) possess multifractal structures from which distinctive spatio-temporal signatures can be extracted as a fingerprint for DS source authentication [2]. Inspired by this finding, the proposed model-free cybersecurity defense framework (shown in Fig. 1) contains three major steps: (1) Analogous Multifractal Height Cross-Correlation Analysis (AMFHXA) is performed on the DS to quantify the long-term cross-correlation of DS from different locations within a distribution network. (2) Weighted Multifractal Surface Interpolation (WMFSI) is developed to reconstruct quasi high-resolution DS by using the derived cross-correlation. (3) Informative spatial and temporal signatures are extracted from the interpolated DS and they are further integrated with RFC for identifying DS source locations.

A. Model of "Source ID Mix" Spoofing Attacks

Considering *a DS measurement matrix as* (1)

$$\mathbf{U} = [U_1, U_2, \cdots U_m] = \begin{bmatrix} u_{1,1} & u_{2,1} & \cdots & u_{m,1} \\ u_{1,2} & u_{2,2} & \cdots & u_{m,2} \\ u_{1,j} & u_{2,j} & \cdots & u_{m,j} \\ u_{1,N} & u_{2,N} & \cdots & u_{m,N} \end{bmatrix} \quad (1)$$

where $u_{i,j}$ denotes the DS measurement from i-th PMU at time instance j. N is the total length of DS measurements and m is the number of PMUs.

For DS data from k-th ($1 \leq k \leq m$) PMU U_k, the "Source ID Mix" attack happens on U_k when U_k is replaced by DS data from i-th ($1 \leq i \leq m$, $i \neq k$) PMU during the same time interval.

B. AMFHXA of Frequency Variations

AMFHXA provides a novel criterion to examine the long-term cross-correlation between pairwise signals [8]. Different from the traditional Pearson Correlation Coefficient (PCC) which evaluates the correlation at a single scale and thus may not be able to detect the "Source ID Mix" data spoofing (since the spoofed data are still within an acceptable range creating minor changes in the correlation coefficients), AMFHXA quantifies the cross-correlation of pairwise time-series data at different temporal scales. For frequency measurements from multiple locations, a high pass filter is first applied to remove the general frequency trend and only preserve the frequency variations [2]. Considering frequency variations $\{U_t\}$ and $\{V_t\}$recorded at two locations, $t = 1, 2, \cdots N$, N is the sample number of frequency variations. The first step of AMFHXA is to construct a cumulative frequency deviation sequence as (2).

$$U(t) = \sum_{i=1}^{t}\left(U_t - \bar{U}\right), V(t) = \sum_{i=1}^{t}\left(V_t - \bar{V}\right) \quad (2)$$

where $\bar{U}$ and $\bar{V}$ are average values of frequency variations.

Then the cross-increment of these two cumulative frequency deviation sequence with time delay L is defined as (3).

$$\Delta_L U(t)V(t) = [U(t) - U(t+L)] \bullet [V(t) - V(t+L)] \quad (3)$$

Subsequently, the q-th order height-height covariance of these two frequency variations is calculated as (4).

$$Cov_{U,V}^{q}(L) = \frac{1}{N-L}\sum_{t=1}^{N-L} sgn[\Delta_L U(t)V(t)] \bullet | \Delta_L U(t)V(t)|^{q/2}, q > 0 \quad (4)$$

The order q examines the varying degrees of frequency variations with small and large magnitude. Normally, the order q less than one magnifies the contribution of variations with small magnitude while the order q above two concentrates on the contribution of variations with large magnitude. In this paper, the 2nd order statistics of fluctuations is adopted which quantifies the cross-correlation of fluctuations with all magnitudes. Based on (4), the AMFHXA coefficient $\rho_q(L)$is calculated as (5), which provides an effective measure to quantify the cross-correlation between two frequency variations at different fluctuation orders and time delay.

$$\rho_q(L) = \frac{Cov_{U,V}^{q}(L)}{\sqrt{Cov_{U,U}^{q}(L) Cov_{V,V}^{q}(L)}}, q = 2, \rho_q(L) \in [-1, 1]. \quad (5)$$

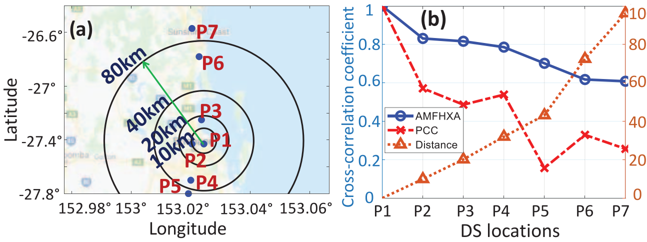

Fig. 2. (a) Locations of frequency signals collected from Queensland network and (b) cross-correlation coefficients between P1 and other six locations.

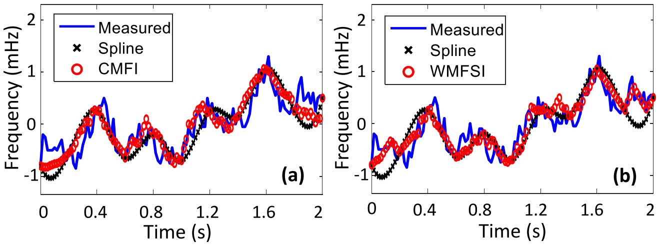

Fig. 3. Interpolation of frequency variations using (a) conventional multi-fractal interpolation and (b) proposed WMFSI method.

C. Weighted Multifractal Surface Interpolation (WMFSI)

Once the AMFHXA coefficient is determined, WMFSI is developed to reconstruct quasi high-resolution frequency variations of each measurement location by maintaining the self-affined and time-invariant structures of the original signal. For WMFSI, frequency variations of a specific location are selected as the target location while frequency variations of the rest locations are used as candidate locations. Then, the 2nd order AMFHXA coefficients between each of the candidate location and target location are calculated. For each pair of candidate and target location, the original frequency variations of the target location are interpolated through two-dimensional multifractal surface interpolation [9] after k iterations which boosts the reporting rate k^2 times higher than the original signal. Then the weighted summation of the interpolated frequency variations by each pair of candidate and target location with the corresponding absolute values of AMFHXA coefficients$|\rho_2|$ as weights is computed. Finally, the above weighted summation is further divided by the summation of weights to generate the quasi high-resolution frequency variation of the target location. In this way, if the frequency variations between the candidate location and target location are highly correlated ($\rho_2 = \pm 1$), a large weight is assigned to the interpolated frequency variations by using this candidate location. In contrast, if the candidate location and target location is uncorrelated ($\rho_2 = 0$), the interpolated frequency variations by using this candidate location are excluded in the final interpolation results.

D. Spatio-Temporal Signature Extraction and Source Authentication

After constructing the quasi high-resolution frequency variations at each location, distinctive spatio-temporal signatures are extracted using the method proposed in [10]. This method extracts the informative features by examining the statistical characteristics, non-stationarity and nonlinearity nature and recurrence characteristics of frequency variations. The extracted spatio-temporal signatures are further used as input features for RFC to recognize the source information of DS measurements.

III. Case Study and Results Discussion

A. Experiment Database Construction and Setup

In this paper, DS from seven locations within a distribution network (denoted as *P1* to *P7* in Fig. 2) over three months are collected. The distance among most measurement locations is within 40km, which are considered as dense locations compared with existing studies where most PMUs are deployed more than 100km far away. For each location, 1000 fragments with 20 seconds length are randomly selected to construct an experimental dataset. This exactly simulates the "Source ID Mix" spoofing attack on short DS fragments at dense locations. The original reporting rate of DS is 50 data points per second. The experiment dataset is further grouped into a training and testing dataset by using 80% and 20% of the samples. The identification rate of the testing samples (the percentage of corrected classified testing samples) is selected as the performance evaluation criterion.

Fig. 2(b) shows an example of cross-correlation coefficients calculated by AMFHXA and PCC using *P1* as the target location. It is clear that the coefficients calculated by AMFHXA gradually decrease when the candidate locations move far away from *P1*. Compared with AMFHXA, the conventional PCC fails to describe such a correlation as the coefficients at some locations significantly diverge from the main trend. In addition, most coefficients calculated by PCC are lower than 0.5 which indicate less correlation among these locations.

B. Results of WMFSI

To demonstrate the performance of the proposed WMFSI approach, Fig. 3 shows an example of two-seconds measured and the interpolated frequency variations using the conventional one-dimension multifractal interpolation (CMFI) [11] and the proposed WMFSI method. The original frequency variations with 50Hz reporting rate are first downsampled to 10 Hz. Then it is interpolated back to 50Hz resolution to make a comparison with the original frequency variations. The interpolation is also performed by using the spline method for comparison purposes.

From Fig. 3 it is observed that the WMFSI shows good performance in reconstructing the frequency variations, where most large variations of the frequency signal can be recovered. In contrast, the spline interpolation can only capture the general trend of the frequency over the whole period and smooth the frequency variations. From Fig. 3(a) and Fig. 3(b) it is found that compared with the conventional multifractal interpolation, the signal processed by the proposed WMFSI shows a higher agreement with the actual measurements. This is because the conventional multifractal interpolation only realizes the multifractal structures using the historical frequency variations of the target location while the proposed method

TABLE I
COMPARISON OF IDENTIFICATION RATE WITH FIVE OTHER ALGORITHMS

Model	**Discrete wavelet transform -ANN**	**Time-frequency mapping-DF**	**Time-frequency mapping-RFC**
Accuracy	54%	81%	80%
Model	**Ensemble empirical mode decomposition - ANN**	**Continuous wavelet transform-CNN**	**Proposed**
Accuracy	85%	88%	93%

TABLE II
IDENTIFICATION RATE WITH DIFFERENT WMFSI RESOLUTION

DS Resolution (Hz)	**200**	**450**	**800**	**1250**	**1800**
Identification rate (%)	83	85	89	93	89

incorporates more information from the neighboring locations which are highly correlated with the target location. For the source identification experiment presented in this paper, 1250Hz is selected as the reporting rate of the frequency variations after WMFSI by considering the computational complexity and identification rate.

C. Performance Evaluation

In this section, the performance of the proposed cybersecurity defense method is compared with other five recently reported algorithms in identifying the source information of DS recorded at seven locations. It is clear that the proposed method outperforms existing methods with an overall identification rate of 93%. Such a high identification rate is mainly because the WMFSI has the capability to further increase the sampling rate of original DS data so that the distinctive spatial-temporal signatures at the high-frequency band can be further realized by the machine learning algorithm for accurate source authentication.

D. Impact of WMFSI Resolution of DS on Identification Rate

The resolution of the frequency variations reconstructed by the proposed WMFSI method has significant impacts on the source identification rate. If the resolution is low, the spatio-temporal signatures may not be fully realized thus making the RFC confuse the source locations of testing samples. However, if the resolution is too high, some values of the extracted spatio-temporal signatures are averaged out which also reduces the identification rate of RFC. By observing the dependency between the resolution and the identification rate in Table II, it is clear that 1250Hz reporting rate is an optimal value for 20-seconds frequency fragments which attains the highest identification rate of 93%.

E. Discussion on the Practicability of DS Cybersecurity Defense Framework

The proposed method can be implemented as a practical DS cybersecurity defense strategy by the following three steps:

(1) DS database construction and spatial-temporal signature extraction: Sufficient amount of historical normal DS data are recorded to build the DS database. Each DS segment is processed by the proposed AMFHXA and WMFSI which is then used to extract distinctive spatial-temporal signatures.

(2) Offline training: The extracted spatial-temporal signatures are used to train the RFC algorithm which builds a mathematical model that describes the correlation between the signatures and the corresponding source locations. Since the spatial-temporal signatures are usually stable over months, the training of RFC does not have to be performed frequently.

(3) Online DS authentication: Once the new DS data is received by the data server, the well-trained model makes prompt classification (less than 10 milliseconds per sample) on the source location of the new DS data of interest and an early warning is raised if any data exception is identified.

IV. CONCLUSION

To mitigate the risk of critical DS-based applications induced by the sophisticated "Source ID Mix" spoofing attack, this letter proposes a cybersecurity defense framework, which combines AMFHXA, WMFSI, spatio-temporal signature extraction and RFC. The multifractal cross-correlation of DS at multiple intra-state locations was explored which can facilitate RFC in realizing unique spatio-temporal signatures of the DS measurements and identifying the corresponding source information. The comparison with some commonly used cybersecurity defense methods reveals that the proposed method has a stronger capability to detect cyber spoofing attacks by using short fragments. It is expected that the explored multifractality of DS can facilitate in improving the detection rate of other sophisticated spoofing attacks (e.g., time mirroring spoofing, time dilation spoofing, et al) on DS and defending the cybersecurity of smart grids.

REFERENCES

[1] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2218–2234, May 2020.

[2] 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, no. 5, pp. 5807–5818, Sep. 2019.

[3] 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, no. 3, pp. 2732–2735, May 2021.

[4] S. Liu *et al.*, "Model-free data authentication for cyber security in power systems," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 4565–4568, Sep. 2020.

[5] Y. Cui, F. Bai, Y. Liu, and Y. Liu, "A measurement source authentication methodology for power system cyber security enhancement," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3914–3916, Jul. 2018.

[6] W. Qiu, Q. Tang, Y. Wang, L. Zhan, Y. Liu, and W. Yao, "Multi-view convolutional neural network for data spoofing cyber-attack detection in distribution synchrophasors," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 3457–3468, Jul. 2020.

[7] W. Qiu *et al.*, "Time-frequency based cyber security defense of wide-area control system for fast frequency reserve," *Int. J. Electr. Power Energy Syst.*, vol. 132, Nov. 2021, Art. no. 107151.

[8] F. Wang, L. Wang, and Y. Chen, "Quantifying the range of cross-correlated fluctuations using a Q-L dependent AHXA coefficient," *Physica A.*, vol. 494, pp. 454–464, Mar. 2018.

[9] H. Sun, "A practical MATLAB program for multifractal interpolation surface," in *Proc. Int. Conf. Nat. Comput.*, 2012, pp. 1–5.

[10] Y. Cui, L. Liu, P. Fuhr, and M. Morales-Rodriguez, "Exploiting spatial signatures of power ENF signal for measurement source authentication," in *Proc. IEEE Int. Symp. Technol. Homeland Security*, 2018, pp. 1–5.

[11] M. F. Barnsley, *Fractals Everywhere*. New York, NY, USA: Dover Publications, 2012.