Source Authentication of Distribution Synchrophasors for Cybersecurity of Microgrids

Source Authentication of Distribution Synchrophasors for Cybersecurity of Microgrids

Yi Cui, *Senior Member, IEEE*, Feifei Bai, *Senior Member, IEEE,* Ruifeng Yan, *Member, IEEE,* Tapan Saha, *Fellow IEEE,* Ryan K L Ko, *Member, IEEE,* Yilu Liu, *Fellow IEEE*

***Abstract*-This letter proposes a hybrid approach combining Self-Adaptive Mathematical Morphology (SAMM) and Time-Frequency (TF) techniques to authenticate the source information of Distribution Synchrophasors (DS) within near-range locations. The SAMM can adaptively regulate the synchrophasors variations which are representatives of local environmental characteristics. Subsequently, TF mapping is employed to extract informative signatures from the regulated synchrophasors variation. Finally, Random Forest Classification (RFC) is used to correlate the extracted signatures with the source information based on the derived TF mapping. Experiment results using DS collected at multiple small geographical scales validated the proposed methodology.**

***Index Terms*- Distribution network, cyber-physical security, synchrophasors, source authentication.**

I. Introduction

The cybersecurity vulnerabilities introduced by the increased digitization of DS and their dependency on information and communication technologies has raised concerns for the security of cyber-physical power systems. Security is particularly important for the microgrid since many advanced applications in the energy management system are based on the DS of distributed energy resources collected within the same grid [1]. Therefore, a measurement Source Authentication (SA) is urgently needed to ensure the data integrity of DS before the data become actionable signals.

"Source ID Mix" data spoofing attack on DS has been identified as a newly-emerging threat to the cybersecurity of the power grid due to its wide impacts and its complexity [2]. It assumes the adversary can manipulate the source information of DS without changing the measurement values. Altering the source information of DS may jeopardize critical synchrophasor-based control and applications, such as wide-area damping control and disturbance localization [2]. In response to the cybersecurity challenges presented by DS, some research efforts have been devoted to the source authentication of DS through two major paths, i.e. model-based methods and data-driven approaches [3]. For model-based methods, SA can be achieved through weighted least squares [4], distributed Kalman filter [5], matrix separation [6] and multi-agent systems [7]. However, these model-based methods face drawbacks due to the need for a detailed system model and accurate parameters, as well as the high computational complexity during the power system state estimation. To overcome the above drawbacks of the model-based SA schemes, data-driven SA schemes have been developed by associating the spatial signatures embedded in the DS with each local grid using support vector machine [8], Neural Networks (NN) [9], RFC [10] and Convolutional Neural Network (CNN) [11-12]. Currently, most SA schemes are developed and validated based on the real-life DS collected at relatively large geographical scales, such as different countries, different interconnections or different feeders within a city, where DS from these far-away locations (i.e. tens to thousands of kilometers) possess distinctive spatial signatures. However, when DS are measured at near-range locations, such as the same feeder or even the same circuit, it would pose significant difficulties for the SA schemes to achieve high identification accuracy due to the high similarity of variations of the measured DS [13]. To our best knowledge, there is no study on the source identification of DS at near-range locations, and the geographical resolution limitation for DS location identification is still unclear.

Our previous studies [10, 14] have found that frequency variation is the natural responses between load and generation changes in each local grid. The peak distribution of the frequency variation possesses distinctive location-specific signatures that can be used as a fingerprint for source identification. Different from previous studies of the authors, in this letter, a hybridized SAMM-TF mapping-based approach is proposed to capture the significant peaks in the highly similar DS measured at multiple near-range locations within a distribution power grid and subsequently extract location-dependent signatures for source identification and authentication. The findings of the study have the potential to improve the understanding of whether or not DS possess distinct location-specific characteristics at small geographical scale, which can be further exploited towards building SA strategies for microgrid data integrity improvement.

II. Proposed Source Authentication Scheme

Fig. 1 shows the overall flowchart of the proposed SA approach, which consists of three steps: (1) A high-pass filter is developed to extract frequency variation of the original DS data; (2) A SAMM-TF mapping-based approach is developed to extract informative features from the synchrophasors variation, which are representatives of local environmental characteristics; (3) The extracted signatures are integrated with RFC algorithm for source authentication.

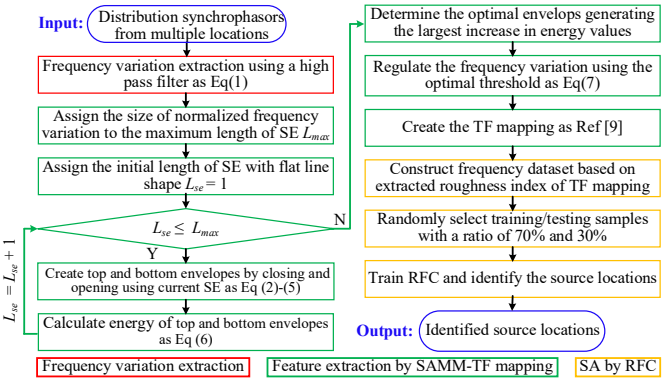


Fig. 1 Flowchart of the proposed SA scheme.

Corresponding author: Feifei Bai (e-mail: f.bai@uq.edu.au). Yi Cui, Feifei Bai, Ruifeng Yan, Tapan Saha and Ryan Ko are with School of Information Technology and Electrical Engineering, The University of Queensland, Brisbane, 4072, Australia (e-mail: y.cui3@uq.edu.au, f.bai@uq.edu.au, ruifeng@itee.uq.edu.au, saha@itee.uq.edu.au, ryan.ko@uq.edu.au).

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

A. Frequency Variation Extraction

In this step, the measured frequency signal is first passed through a weighted high pass filter to capture the main trend of the frequency signal. Such a trend is further subtracted from the original frequency data to extract the variation from the frequency signal as (1).

$$S_{hp}(t) = S(t) - \sum_{i=-(K-1)/2}^{(K-1)/2} \omega_i S(t-i) \quad (1)$$

where $S(t)$ and $S_{hp}(t)$ denote the original frequency signal and extracted frequency variation from a specific location, ω_i denotes the weights of the high pass filter which is the convolution of the vector $[0.5 \ \cdots \ 0.5]$ with K elements, K is the order of the filter and it is selected as an odd number.

B. Feature Extraction using Self-Adaptive Mathematical Morphology (SAMM) and Time-Frequency (TF) Mapping

After the frequency variation extraction, SAMM is implemented to regulate the frequency variations by which the peaks of the extracted variations with large magnitude and sufficient interval are preserved. In SAMM, the extracted frequency variation is first normalized between [-1, 1]. Unlike wavelet-based methods which require careful selection of mother wavelet and decomposition level, the shape of structural elements (SE) in SAMM does not affect signal analysis much [15]. Therefore, SE with a flat line shape and an initial length of 1 is used due to its simplicity in processing without considering its amplitude. Then closing ($\bullet$) and opening ($\circ$) operations using the SE are performed on the normalized frequency variation through two fundamental dilation ($\oplus$) and erosion (Θ) operations to generate top and bottom envelopes, respectively as (2)-(5).

$$\left(S_{hp} \oplus E\right)_n = \max\left[S_{hp}(n-m) + E(m)\right], n-m \geq 0, m \geq 0 \quad (2)$$

$$\left(S_{hp} \Theta E\right)_n = \min\left[S_{hp}(n+m) - E(m)\right], n+m \geq 0, m \geq 0 \quad (3)$$

$$\left(S_{hp} \circ E\right)_n = \left[\left(S_{hp} \Theta E\right) \oplus E\right]_n \quad (4)$$

$$\left(S_{hp} \bullet E\right)_n = \left[\left(S_{hp} \oplus E\right) \Theta E\right]_n \quad (5)$$

where E denotes the SE as a vector with length m, n is the sample size of frequency variation.

Afterwards, energy of the top (e_{top}) and bottom envelops (e_{bottom}) is calculated using (6).

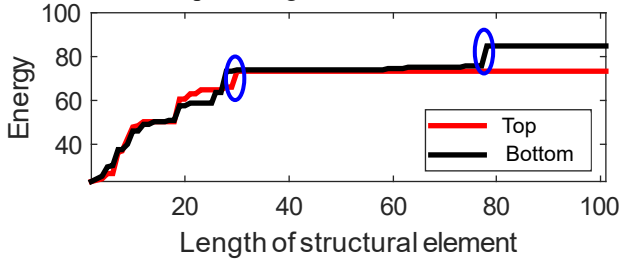
$$e_{top} = \sum_{i=1}^{n}\left[\left(S_{hp} \bullet E\right)_i\right]^2, e_{bottom} = \sum_{i=1}^{n}\left[\left(S_{hp} \circ E\right)_i\right]^2 \quad (6)$$

The length of the SE increases by 1 and the above procedures are repeated until the length of the SE reaches the number of data points of the frequency variation signal. With the increase in the SE length, more peaks are preserved and the energy of the envelopes also increases. However, if the envelopes contain the peaks with small intervals or the peaks with large intervals but small magnitudes, the energy will not grow significantly (middle part of Fig. 2a). In contrast, for envelopes containing more peaks with long intervals and large magnitude, energy will grow significantly (marked as blue circles in Fig. 2a). Then the top/bottom envelopes which create the largest increase in the energy are selected as optimal envelopes and the optimal threshold is calculated as the mean values of the optimal envelopes. Finally, hard thresholding is applied to the positive and negative frequency variation using the optimal top and bottom threshold (Fig. 2b) so that peaks with large magnitude and sufficient interval are preserved as (7).

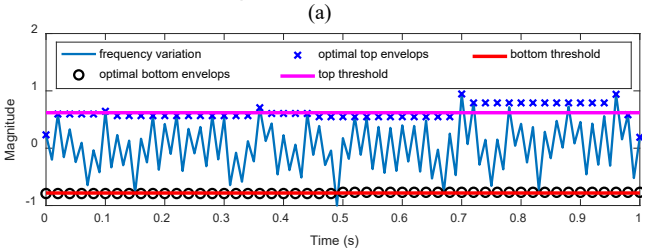
$$S_{sp}^{'} = \begin{cases} 1 & S_{hp} > 0, S_{hp} > T_{top} \\ -1 & S_{hp} < 0, S_{hp} < T_{bottom} \\ 0 & otherwise \end{cases} \quad (7)$$

where $S_{sp}^{'}$ denotes frequency variation after SAMM, T_{top} and T_{bottom} denote the optimal top and bottom threshold.

After signal regulation through SAMM, TF mapping (detailed in [10]) is implemented which calculates the peak sparsity trend of a signal in time and frequency domains. It transforms a signal from the time domain to a two-dimensional plane by using the sparsity trend and roughness index so that the samples are distinguishable. The sparsity trend and roughness index of the regulated frequency variation are used as location-specific signatures for source authentication.



(a)



(b)

Fig. 2 Example of SAMM on a normalized frequency variation signal. (a) Energy of top/bottom envelops, and (b) Optimal top (blue crosses) and bottom envelopes (black circles), and corresponding optimal thresholds (pink and red lines).

III. Methodology Verification

A. Frequency Database Construction and Experiment Setup

To investigate the performance of the proposed SA scheme, two case studies are presented which simulate the "Source ID Mix" attack on DS collected at different geographical scales. The first case study identifies the source locations of DS measured at three locations in the same feeder of a distribution network, while the second case study recognizes the source locations of DS from five rooms in the same building (circuit). Given that the frequency response of an electromechanical disturbance usually lasts for tens of seconds, for each case study, 1000 frequency segments with each having 10 seconds length are randomly selected from each location in three consecutive months for constructing the frequency dataset. The reporting rate of the DS is 100Hz. 70% of the samples are chosen as the training dataset and the remaining 30% are used for evaluating the authentication performance. The above procedures are repeated for 30 rounds and the average match accuracy (i.e. ratio between the number of correctly identified testing samples and the total number of testing samples) is calculated as the evaluation metric.

B. Results of 3-Location Data from the Same Feeder

In this case study, the frequency signals are measured at three nodes (*P1-P3*) in the same feeder of the University of Queensland (UQ), which is shown in Fig. 3. Two rooftop Photovoltaics (PVs) are installed at *P2* and *P3*. The distance

among different locations is just hundreds of meters.

Fig. 4 compares the original normalized frequency variation from two locations and the frequency variation processed by the proposed SAMM. It is evident that the original normalized frequency variation of these two locations has a high similarity which may create significant difficulties in separating the source locations. The proposed SAMM can adaptively preserve the significant peaks so that distinguishing signatures can be extracted from the regulated signals for source authentication. From TABLE I it is clear that the proposed method shows good performance in recognizing the source locations of the testing samples with an overall match accuracy of 96%, as compared to other techniques as discussed in Section III.D and TABLE III.

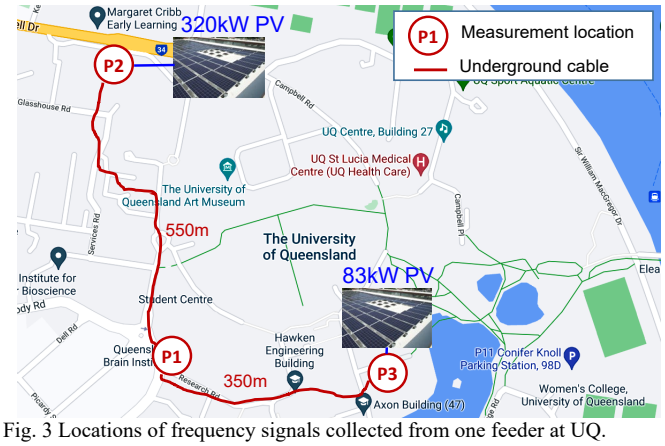


Fig. 3 Locations of frequency signals collected from one feeder at UQ.

TABLE I
IDENTIFICATION RESULTS OF FREQUENCY SIGNALS FROM THE SAME FEEDER

MATCH ACCURACY (%)	P1	P2	P3	Overall
	100	91	97	96

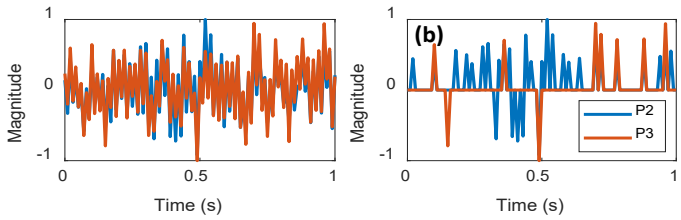


Fig. 4 Comparison of (a) normalized frequency variation and (b) frequency variation after SAMM processing from two locations in the same feeder.

C. Results of 5-Location Data from the Same Building

In this case study, the frequency signals are collected at five rooms (*R1-R5* in Fig. 5) in the same building. During the experiment, it is noticed that by using a single classifier, the match accuracy of the frequency signals is low. Further examination on classification results shows that it is mainly due to the low training accuracy of the RFC. This is not surprising since the locations of frequency recordings are close to each other and minimum difference would exist in the frequency measurement thus making the single classifier hard to correctly separate frequency signals with high similarities.

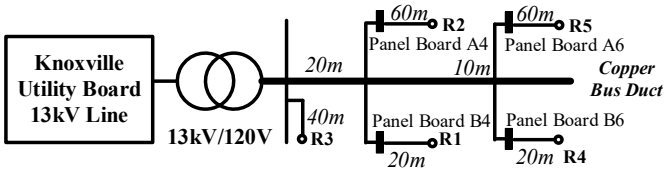


Fig. 5 Locations of frequency signals collected from one building.

To improve the training accuracy of the classifier and the subsequent match accuracy of the testing samples, Adaptive Boosting (AdaBoost) technique is employed which can "boost" the performance of classification algorithms by combining the outputs from different classifiers. The fundamental of AdaBoost is that multiple under-performance classifiers (termed as weak classifiers) can be aggregated to form a high-performance ensemble (termed as a strong classifier). During the training of the first weak classifier, all the training samples are assigned with equal weights. Then the training samples which are not correctly classified by the first weak classifier are given higher weights to redirect the subsequent weak classifier to focus on these samples. The training accuracy and the classification outputs of each weak classifier on the testing samples are also recorded and the number of aggregated weak classifiers will increase until the ensemble of all weak learners attains the desirable training accuracy. Finally, the classification results of the testing samples can be determined by aggregating the outputs from all weak classifiers. From TABLE II it shows the overall testing accuracy reaches 90% by using AdaBoost.

TABLE II
IDENTIFICATION RESULTS OF FREQUENCY SIGNALS FROM THE SAME BUILDING

MATCH ACCURACY (%)	R1	R2	R3	R4	R5	Overall
	100	80	100	80	93.4	90.68

D. Statistical Analysis of other Source Authentication Schemes

In this section, a statistical comparison is performed by applying the recently published four SA schemes on the 3-location data from the same feeder. It shows the proposed SAMM-TF-RFC algorithm attains the highest identification accuracy compared with the rest four SA schemes.

TABLE III
COMPARISON OF IDENTIFICATION ACCURACY WITH OTHER FOUR ALGORITHMS

Ref	[10]	[2]	[14]	[9]	Proposed
Method	MM-TF-RFC	MM-TF-gcForest	DWT-NN	EEMD-NN	SAMM-TF-RFC
Accuracy (%)	77	76	76	88	96

IV. CONCLUSION

This letter proposes a source authentication methodology, which is a hybrid of SAMM, TF mapping and RFC. The proposed method can achieve high accuracy in recognizing the source information of distribution synchrophasors measured at multiple locations of the same feeder or even the same circuit, where high similarity is presented in the measured data. Compared with previous methods, higher identification accuracy can be achieved by the proposed method using much less data, which has the potential to provide system operators with critical insights over legitimate data patterns used in detecting abnormal patterns and build source authentication strategies for microgrid cybersecurity enhancement.

ACKNOWLEDGMENT

This work was supported in part by the University of Queensland Solar, Australia (UQ Solar; solar-energy.uq.edu.au), in part by the Advance Queensland Platform Technology Program AQPTP01216-17RD1, in part by the Queensland State Government, Australia under the Advance Queensland Research Fellowship AQIRF0022018 and in part by the Engineering Research Centre Program of the National Science Foundation and the Department of Energy under NSF Award Number EEC-1041877 and the CURENT Industry Partnership Program.

REFERENCES

[1] J. Qi, A. Hahn, X. Lu, J. Wang and C. Liu, "Cybersecurity for Distributed Energy Resources and Smart Inverters," *IET Cyber-Physical Systems: Theory & Applications*, vol.1, Issue 1, pp. 28-39, 2016.

[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, Issue 5, pp. 5807-5818, 2019.

[3] 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, Issue 3, pp. 2218-2234, 2020.

[4] J. Duan, W. Zeng and M. Chow, "Resilient Distributed DC Optimal Power Flow Against Data Integrity Attack," *IEEE Trans. Smart Grid*, vol.9, Issue 4, pp. 3543-3552, 2018.

[5] A. S. Musleh, H. M. Khalid, S. M. Muyeen and A. Al-Durra, "A Prediction Algorithm to Enhance Grid Resilience Toward Cyber Attacks in WAMCS Applications," *IEEE Syst. J.*, vol.13, Issue 1, pp. 710-719, 2019.

[6] B. Li, T. Ding, C. Huang, J. Zhao, Y. Yang and Y. Chen, "Detecting False Data Injection Attacks Against Power System State Estimation with Fast Go-Decomposition Approach," *IEEE Trans. Ind. Inf.*, vol.15, Issue 5, pp. 2892-2904, 2019.

[7] T. R. B. Kushal, K. Lai and M. S. Illindala, "Risk-Based Mitigation of Load Curtailment Cyber Attack Using Intelligent Agents in a Shipboard Power System," *IEEE Trans. Smart Grid*, vol.10, Issue 5, pp. 4741-4750, 2019.

[8] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng and Z. Han, "Detecting Stealthy False Data Injection Using Machine Learning in Smart Grid," *IEEE Syst. J.*, vol.11, Issue 3, pp. 1644-1652, 2017.

[9] 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.

[10] 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.

[11] W. Qiu, Q. Tang, K. Zhu, W. Wang, Y. Liu and W. Yao, "Detection of Synchrophasor False Data Injection Attack using Feature Interactive Network," *IEEE Transactions on Smart Grid (early access)*, 2020, DOI:10.1109/TSG.2020.3014311.

[12] 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, Issue 4, pp. 3457-3468, 2020.

[13] R. Garg, A. Hajj-Ahmad and M. Wu, "Geo-Location Estimation From Electrical Network Frequency Signals," *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2013, pp. 1-5.

[14] 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.

[15] Y. Dong, M. Liao, X. Zhang and F. Wang, "Faults Diagnosis of Rolling Element Bearings Based On Modified Morphological Method," *Mech. Syst. Sig. Process.*, vol.25, Issue 4, pp. 1276-1286, 2011.