Model-free Data Authentication for Cyber Security in Power Systems

Shengyuan Liu, Shutang You, *Member, IEEE*, He Yin, *Member, IEEE*, Zhenzhi Lin, *Member, IEEE*, Yilu Liu, *Fellow, IEEE*, Wenxuan Yao, *Member, IEEE*, Lakshmi Sundaresh

***Abstract*—With the development and wide deployment of measurement equipment, data can be automatically measured and visualized for situation awareness in power systems. However, the cyber security of power systems is also threated by data spoofing attacks. This letter proposed a measurement data source authentication (MDSA) algorithm based on feature extraction techniques including ensemble empirical mode decomposition (EEMD) and fast Fourier transform (FFT), and machine learning for real-time measurement data classification. Compared with previous work, the proposed algorithm can achieve higher accuracy of MDSA using a shorter window of data from closely located synchrophasor measurement sensors.**

***Index Terms*—cyber security, data authentication, ensemble empirical mode decomposition (EEMD), fast Fourier transform (FFT), back propagation (BP) network.**

I. Introduction

Modern power systems are typical highly-dynamic real-time cyber-physical systems (CPS) with complex interdependencies and interactions between power components and information infrastructure, and the security and authentication of measurement data are attracting more and more attention from power system operators and reliability regulators. Frequency measurement is very useful for power system data authentication since the frequency is a system-wide attribute and its intrinsic real-time characteristic automatically verifies its authenticity in the time domain. This feature of frequency data has been applied in some applications such as audio authentication [1]. However, it is extremely challenging to authenticate it in the spatial domain. Recently, a type of data spoofing attack called data source ID mix attack was discovered, and some algorithms to authenticate the data source and detect this attack have been proposed. In [2]-[4], algorithms based on principal component analysis (PCA), support vector machine (SVM), state estimation and Kalman filter (KF) are studied respectively to detect false data injection. As all these algorithms need detailed and accurate electrical parameters of the whole power system, this requirement places a strict prerequisite in the practical and online application. In [5], wavelet transform and feed-forward artificial neural network (F-ANN) are utilized to perform location identification for electric network frequency (ENF), and this algorithm achieves high accuracy of measurement data source authentication (MDSA) for the frequency disturbance recorders (FDRs) located far away from each other. In [6] and [7], mathematical morphology (MM) and advanced multi-grained cascade forest (gcForest) technique are combined to detect source ID mix using a long-time period of FDR data, and the results show that the algorithm can obtain a high accuracy of MDSA for FDRs located nearly. However, the aforementioned algorithms have obvious limitations. For the algorithm proposed in [5], the average source identification accuracy for FDRs located in the same city is lower than 50%. For the algorithms presented in [6] and [7], quite a long time window (e.g. 10min) of data is required to authenticate the data source.

This work proposes a practical data spoofing detection solution based on ensemble empirical mode decomposition (EEMD), fast Fourier transform (FFT) and 2-hidden-layers back propagation (BP) neural network. The high-reporting-rate synchrophasor data from universal grid analyzers (UGAs) are used for the first time. Contributions of this work include:

i) An algorithm based on EEMD, FFT and BP network is proposed to perform MDSA. Compared with previous work, this data-driven algorithm has three advantages: it does not need detailed electrical parameters of power systems; achieves a higher accuracy (e.g. >80%) of MDSA; and significantly shortens the time window required for data authentication.

ii) The sensitivity of the accuracy of MDSA on the data reporting rate, time window length, and the number of layers in BP network are studied in details to provide a guideline on parameter settings for MDSA to achieve higher accuracy with shorter time period in practical application

II. Practical MDSA Using High-speed UGAs

FNET/GridEye is a wide-area monitoring system deployed worldwide to improve situational awareness in power systems. In this study, the latest version of FDRs (i.e., UGAs) [8] with a high data reporting rate (up to 1.44kHz) is used to measure frequency in power systems. To authenticate the UGA frequency measurements at different locations, EEMD is employed to first extract the intrinsic mode functions (IMFs) of each data source. An IMF is a mutually independent oscillatory function with time-varying frequencies that contain the local

Shengyuan Liu is with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996, USA, while on leave from Zhejiang University, China (e-mail: eelsy@zju.edu.cn).

Zhenzhi Lin is with the College of Electrical Engineering, Zhejiang University, Hangzhou 310027, China (e-mail: linzhenzhi@zju.edu.cn).

Shutang You, He Yin, Wenxuan Yao, and Lakshmi Sundaresh are with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996 USA (e-mails: syou3@utk.edu; hyin8@utk.edu; wyao3@vols.utk.edu; lsundare@vols.utk.edu).

Yilu Liu is with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN, 37996, USA and also with Oak Ridge National Laboratory, Oak Ridge, TN, 37830, USA (email: liu@utk.edu)

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2020.2986704, IEEE Transactions on Smart Grid

characteristics of non-stationary signals at different time scales. It is defined as a function that satisfies the requirements: i) the numbers of extremums and zero-crossing points must either be equal or differ at most by one; ii) At any point, the mean value of the envelope defined by the local maximum and the envelope defined by the local minimum is zero [9], [10]. In summary, IMF represents an oscillatory mode as a simple harmonic function, which can be any function with symmetric envelopes for zero and the same number of extremums and zero-crossing points. Then, the FFT is utilized to analyze the frequency spectrum of IMFs and extract features of each data source. Afterward, a 2-layer BP neural network is trained and applied to authenticate the source of real-time measurement data. Assume an observation of the i^{th} data source is represented as

$$\boldsymbol{f}_i = [f_{i,1}, f_{i,2}, \ldots, f_{i,N}]^{\mathrm{T}} \tag{1}$$

where N is the number of data points in a given window length L. The value of N is determined by the window length L and the data reporting rate R (i.e. $N=L\times R$). The motivation of EEMD is to decompose the frequency data into several IMFs. Compared with the traditional empirical mode decomposition (EMD), it can avoid the mode mixing problem [11]. The sifting procedure of EEMD for the i^{th} data source are as follows.

1) Set loop variables j=1 and k=1.
2) Add the k^{th} type of Gaussian white noise $\boldsymbol{\zeta}^k$ into the original frequency data as $\boldsymbol{f}_i^k = \boldsymbol{f}_i + \boldsymbol{\zeta}^k$.
3) Find out all the local maxima and minima of $\boldsymbol{f}_i^k$ and connect them to obtain the upper and lower envelope curves $\boldsymbol{f}_i^{k,\mathrm{U}}$ and $\boldsymbol{f}_i^{k,\mathrm{L}}$.
4) Determine the j^{th} IMF of $\boldsymbol{f}_i^k$ as $\boldsymbol{\varphi}_{i,j}^k = \boldsymbol{f}_i^k - (\boldsymbol{f}_i^{k,\mathrm{U}} + \boldsymbol{f}_i^{k,\mathrm{L}})/2$; and $\boldsymbol{f}_i^k = \boldsymbol{\varphi}_{i,j}^k$, j=j+1;
5) Repeat steps 3)-4) if $\boldsymbol{f}_i^k$ is not monotonic; otherwise, let residual $\boldsymbol{r}_i^k = \boldsymbol{f}_i^k$, k=k+1.
6) Repeat steps 2)-5) with different $\boldsymbol{\zeta}_k$ until $k>K$, where K is the number of types of Gaussian white noise utilized in EEMD.
7) The final IMFs $\boldsymbol{\varphi}_{i,j}$ and residual $\boldsymbol{r}_i$ of the i^{th} data source are decomposed from $\boldsymbol{f}_i$ as

$$\boldsymbol{f}_i = \sum_{j=1}^{N_{\mathrm{IMF}_i}} \boldsymbol{\varphi}_{i,j} + \boldsymbol{r}_i \tag{2}$$

where $\boldsymbol{\varphi}_{i,j} = \frac{1}{K}\sum_{k=1}^{K} \boldsymbol{\varphi}_{i,j}^k$, and $\boldsymbol{r}_i = \frac{1}{K}\sum_{k=1}^{K} \boldsymbol{r}_i^k$; N_{IMF_i} is the number of IMFs for the i^{th} data source.

It is worth to mention two points of the above processes that: i) Adding Gaussian noise for $\boldsymbol{f}_i^k$ is one of the most important processes of EEMD. EEMD improves the traditional EMD by avoiding the mode mixing problem [11]. The signal extremums affect IMF, and mode mixing problem occurs if their distributions are uneven. To remedy this deficit, Gaussian noise, whose spectrum is evenly distributed, is involved into the signal to be analyzed so that the signal could have a smaller signal-to-noise ratio, and it will provide a uniform reference scale distribution to extract IMFs. Hence, adding Gaussian noise would not affect EMD but enhances it by avoiding the mode mixing actually [12]. ii) It is proved in [13] that the monotonic function in Step 5) can always be found after several iterations with trigonometric interpolation. In other words, the convergence of the sifting procedure of EEMD can be guaranteed.

After the EEMD, the characteristics of measurement data in various time scales are extracted and represented by IMFs, and FFT is further employed to extract the characteristics in the frequency domain as

$$Y_{i,j}(p) = \sum_{q=1}^{Q} \varphi_{i,j}(q)(w_n)^{(p-1)(q-1)} \tag{3}$$

where $w_n = \mathrm{e}^{-2\pi \mathrm{i}/n}$ and $\varphi_{i,j}(q)$ is the q^{th} element of the sequence $\boldsymbol{\varphi}_{i,j}$. $Y_{i,j}(p)$ is the p^{th} element of the frequency domain representation $\boldsymbol{Y}_{i,j}$. $\boldsymbol{Y}_{i,j}$ is a sequence of P complex numbers whose amplitudes are the spectrums of measured data. In this work, MDSA is a classification problem and BP neural network can solve this problem using its strong nonlinear mapping capability.

Hence, the 2-hidden-layers BP neural network can be built as shown in Fig. 1. The spectrums of measured data extracted by EEMD and FFT are used as the input features to train a classifier of BP neural network and the effectiveness of the proposed algorithm compared with other algorithms is given in Section III.

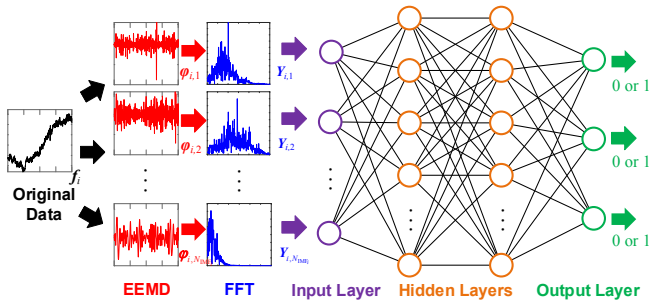

Fig. 1. Architecture and input features of the proposed BP neural network

It should be mentioned that for UGAs with such a high-reporting rate, not only the local characteristics of power systems but also the measurement noises from sensing devices will be recorded and it is difficult to separate them thoroughly in practice. However, the mix of local characteristics and measurement noises would not influence the results of MSDA because both of them reflect the unique characteristics of the data and help to authenticate the data. In other words, the local characteristics are spatial signatures, while the measurement noises are device signatures, and both are used to authenticate the data.

III. Case Studies and Comparisons

To demonstrate the effectiveness of the proposed algorithm, the data of three UGAs deployed closely in Knoxville, TN, USA, are employed for MDSA. These three UGAs are deployed several kilometers away from each other and the physical locations of these three high-speed UGAs are shown in Fig. 2. The measured data are from 2019/07/17 00:00:00 to 2019/07/18 23:59:59 with a 1.44kHz reporting rate. In this work, window length L=20s and a reporting rate R=60Hz are

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2020.2986704, IEEE Transactions on Smart Grid

used, respectively, which is a typical parameter of synchrophasor measurement.

Fig. 2. Locations of UGAs

Thus, EEMD is employed to decompose the original data into several IMFs and the residual. The first three IMFs and the residual are plotted in Fig. 3. It can be seen that IMF_1 has the fastest variations and the residual is monotonic. Hence, the characteristics of original data in different time scales are extracted. FFT is further employed to obtain the characteristics in the frequency domain, which are utilized as the input data of BP neural network.

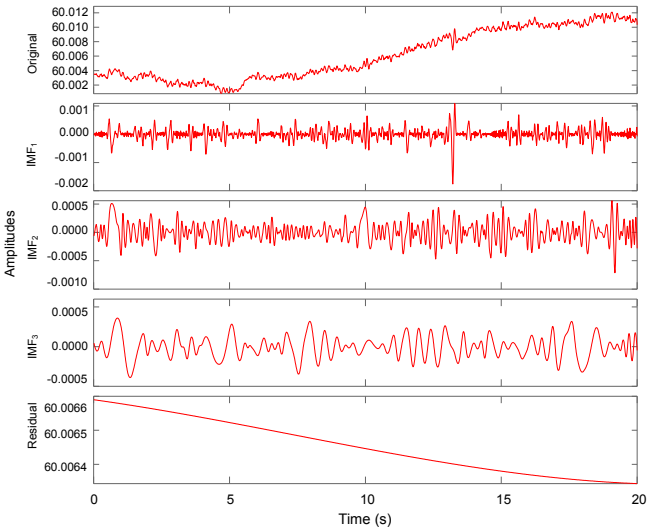

Fig. 3. Results of EEMD for original frequency data with the first three IMFs and residuals.

To verify the algorithm, 70%, 15% and 15% of the whole data are used as the training set, validation set and testing set, respectively. In the testing set, the data sources are mixed, and the verification results are clarified by confusion matrices as shown in Fig. 4. For each confusion matrix, the element in (i, i) denotes the number of times that the i^{th} UGA is correctly authenticated as in the i^{th} location; while the element in (i, j) denotes the number of times that the j^{th} UGA is incorrectly authenticated as in the i^{th} location (i, j=1, 2, 3; $i \neq j$). In other words, the larger the values of the diagonal elements and the smaller the values of the non-diagonal elements, the more accurate the algorithm is. It can be seen that the identification accuracies on training, validation and testing sets are 88.5%, 79.9% and 80.9%, respectively; and the overall accuracy of MDSA on data set is 86.0%. The accuracy of MDSA on the test set is the most meaningful since its value represents the accuracy of MDSA in practical application. The accuracies and training times on the testing set obtained by four other algorithms are also given in Table I for comparisons. It is noted that this case is performed on the Windows 10 platform with Intel Core i5-8250U processor and 8GB RAM. It can be seen that: i) The proposed algorithm earns the highest accuracy of MDSA. ii) The required time window length of the proposed algorithm is much shorter than that of MM-RFC algorithm (i.e., L=10min) reported in [7]. iii) The long short-term memory (LSTM)-based algorithm obtains the second highest accuracy, while its training time is longest due to the more complex network structure. It is also worth mentioning that many parameters in LSTM network need to be tuned to optimize its performance, which makes it less convenient compared with the proposed method for MDSA.

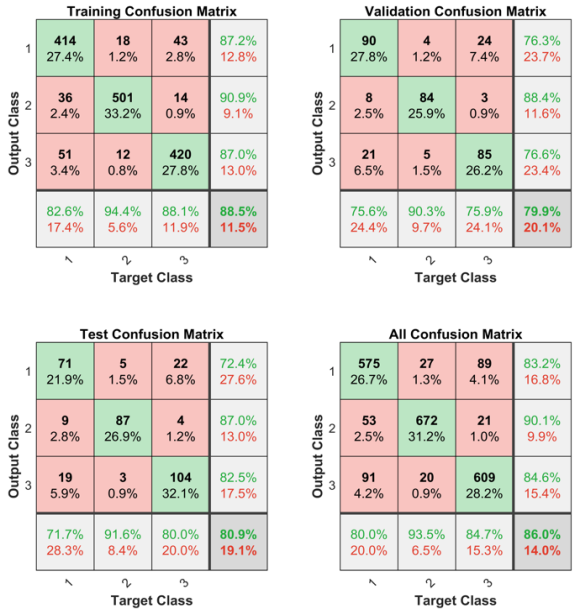

Fig. 4. Confusion matrices of the proposed EEMD-BP algorithm.

TABLE I
ACCURACY AND TRAINING TIME OF DIFFERENT ALGORITHMS

Algorithm	Accuracy	Training Time
DWT-BP [5]	76.5%	6.94s
MM-gcForest [6]	63.7%	4.65s
MM-RFC [7]	66.1%	5.63s
LSTM	77.8%	10.25s
Proposed Algorithm	80.9%	6.64s

In fact, UGAs are not deployed widely in current stage. Therefore, there was no recorded spoofing attack at the time of collecting data and only three UGAs are employed in this work for verification. To demonstrate the effectiveness in large-scale systems with a substantial number of measurements and the real-time application, the data from 54 FDRs in the U.S. Eastern Interconnection grid are utilized. It is assumed that FDRs #10 and #45 are attacked with their data sources swapped intentionally between 22:00:00 to 22:30:00. The real-time monitoring graph is shown in Fig. 6 (for clarity, only the results associated with FDRs #10 and #45 are plotted). The total training time is 13.26s, which indicates that the training time will not increase significantly with the increase of the number of synchrophasors. It can be seen that the locations of FDRs #10 and #45 can be correctly identified when no attack arises at most time. Furthermore, the identified locations of swapped

FDRs after the attack are also exchanged, which indicates an attack that aims to swap the data sources of FDRs #10 and #45 is in progress. Therefore, the attack is detected and identified successfully. It can be seen from this example that the proposed algorithm works well for the system with numerous FDRs. Hence, the proposed algorithm will achieve at least the same performance when it is applied for UGAs, which are with a much higher reporting rate than FDRs.

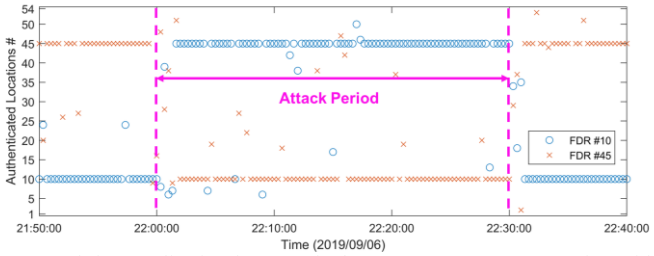

Fig. 6. Real-time application for FDRs in the U.S. Eastern Interconnection grid.

IV. Parameter Sensitivity Study

It is noted that different window lengths, reporting rates and numbers of layers in neural network would result in different identification accuracies. Results of MDSA with different reporting rates and window lengths in 1 and 2-hidden-layer BP networks are given in Table II. It can be seen that: i) For the 10Hz reporting rate, it fails to catch enough features in measurement data for accurate identification; for the 1,440Hz one, some useless features may be included and influence the accuracy of MDSA. ii) 60Hz and 144Hz reporting rate data produce better results than the 10Hz and 1,440Hz data, while the highest accuracy of MDSA is obtained by 144Hz reporting rate. iii) For the 1s and 5s window lengths, their accuracy is relatively low due to insufficient local information in data. Besides, the accuracy of MDSA based on the 60s window length is also low since some features extracted by the proposed algorithm may be averaged. iv) The accuracies obtained by 20s window length are higher than the 1s, 5s and 10s ones. Besides, results obtained by 20s and 40s window lengths are close. v) The results obtained by the 2-hidden layer BP network are generally better than the ones obtained by the 1-hidden layer BP network. Further tests show that 3 or more hidden-layers BP network would bring little improvement but much more computation burden and potentially lead to the overfitting problem. Therefore, the 20s window length with 60Hz reporting rate in the 2-hidden layers BP network is suitable for the proposed algorithm in this test data. As these results provide some guidelines on tuning the algorithm parameter settings, actual settings in practice will fine be tuned based on system characteristics and the electrical distance between sensors.

TABLE II
Results of MDSA with Different Reporting Rates and Window Lengths in 1 and 2-hidden-layer BP Networks

Network	Rates	1s	5s	10s	20s	40s	60s
1-hidden layer	10Hz	36.9%	51.1%	56.0%	50.9%	33.3%	38.0%
	60Hz	50.3%	66.7%	74.7%	77.6%	75.3%	64.8%
	144Hz	58.4%	66.1%	65.7%	64.2%	77.8%	70.4%
	1,440Hz	41.1%	40.8%	26.6%	40.4%	71.0%	63.3%
2-hidden layers	10Hz	43.3%	49.9%	57.7%	65.0%	35.8%	39.8%
	60Hz	52.2%	61.6%	76.2%	**80.9%**	75.9%	73.1%
	144Hz	59.8%	64.3%	72.3%	75.5%	**81.5%**	72.2%
	1,440Hz	42.3%	49.2%	53.0%	70.7%	61.1%	63.0%

V. Conclusions

This work presented a model-free approach for MDSA based on EEMD, FFT and BP neural network. The sensitivity of its accuracy on window length and reporting rates is studied. Compared with previous approaches, more accurate data authentication can be achieved while using data in a much shorter time window, improving the speed and accuracy of detecting data spoofing cyber-attacks.

Acknowledgment

Funding for this research was provided by the NSF Cyber-Physical Systems (CPS) Program under award number 1931975. This work also made use of Engineering Research Center shared facilities supported by the Engineering Research Center Program of the National Science Foundation and the Department of Energy under NSF Award Number EEC-1041877 and the CURENT Industry Partnership Program. The first author is also grateful for the support of China Scholarship Council (CSC).

References

[1] Y. Liu, Z. Yuan, P.N. Markham, R.W. Conners, and Y. Liu, " Application of power system frequency for digital audio authentication," *IEEE Transactions on Power Delivery*, vol. 27, no. 4, pp. 1820-1828, Oct. 2012.

[2] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1644-1652, Sep. 2017.

[3] X. Fan, L. Du and D. Duan, "Synchrophasor data correction under GPS spoofing attack: a state estimation-based approach," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4538-4546, Sep. 2018.

[4] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Transactions on Control of Network Systems*, vol. 1, no. 4, pp. 370-379, Dec. 2014.

[5] 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, May 2017.

[6] Y. Cui, F. Bai, Y. Liu, P. L. Fuhr, and M. E. Morales-Rodriguez, "Spatio-temporal characterization of synchrophasor data against spoofing attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5807-5818, Sep. 2019.

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

[8] H. Yin, W. Yu, A. Bhandari, W. Yao, and L. Zhan, "Advanced universal grid analyzer development and Implementation," *in Proceeding of International Conference on Smart Grid Synchronized Measurements and Analytics*, College Station, TX, USA, 2019.

[9] V. K. Rai and A. R. Mohanty, "Bearing fault diagnosis using FFT of intrinsic mode functions in Hilbert–Huang transform," *Mechanical Systems and Signal Processing*, vol. 21, no. 6, pp.2607-2615, Aug. 2007.

[10] R. B. Pachori and S. Patidar, "Epileptic seizure classification in EEG signals using second-order difference plot of intrinsic mode functions," *Computer Methods and Programs in Biomedicine*, vol. 113, no. 2, pp. 494-502, Feb. 2014.

[11] D. C. Martinez, M. V. Rodriguez, C. A. Ramirez, J. P. Sanchez, R. J. Troncoso, and A. Perez, "Novel downsampling empirical mode decomposition approach for power quality analysis," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 4, pp. 2369-2378, Apr. 2016.

[12] Z. Wu and N. E. Huang, "Ensemble empirical mode decomposition: a noise assisted data analysis method," *Advances in Adaptive Data Analysis*, vol. 1, no. 1, pp. 1-41, Aug. 2005.

[13] S. D. Hawley, L. E. Atlas and H. J. Chizeck, "Some properties of an empirical mode type signal decomposition algorithm," *IEEE Signal Processing Letters*, vol. 17, no. 1, pp. 24-27, Jan. 2010.