Adaptive Hierarchical Cyber Attack Detection and Localization in Active Distribution Systems

Qi Li, *Student Member, IEEE*, Jinan Zhang, *Student Member, IEEE*, Junbo Zhao, *Senior Member, IEEE*, Jin Ye, *Senior Member, IEEE*, WenZhan Song, *Senior Member, IEEE*, Fangyu Li*, *Member, IEEE*

***Abstract*—Development of a cyber security strategy for the active distribution systems is challenging due to the inclusion of distributed renewable energy generations. This paper proposes an adaptive hierarchical cyber attack detection and localization framework for distributed active distribution systems via analyzing electrical waveforms. Cyber attack detection is based on a sequential deep learning model, via which even minor cyber attacks can be identified. The two-stage cyber attack localization algorithm first estimates the cyber attack sub-region, and then localize the specified cyber attack within the estimated sub-region. We propose a modified spectral clustering-based network partitioning method for the hierarchical cyber attack 'coarse' localization. Next, to further narrow down the cyber attack location, a normalized impact score based on waveform statistical metrics is proposed to obtain a 'fine' cyber attack location by characterizing different waveform properties. Finally, compared with classical and state-of-art methods, a comprehensive quantitative evaluation with two case studies shows promising estimation results of the proposed framework.**

***Index Terms*—cyber attack localization, adaptive, hierarchical, online, distribution networks**

I. Introduction

CYBER attack localization is important to protect smart distribution grids, but also a challenging task because of the inherent distributed energy resources (DER) and topology complexities [1], [2]. Raw electrical waveforms, signals of electrical networks, together with those in cyber networks provide great potentials in cyber attack detection [3]. For example, devices in power networks must leave clues of their operational status and health (including faults or attacks) information in the raw electrical waveform signals: a cyber-device in fault or under attack will cause unusual energy consumption pattern in power networks [4]; a power electronics or electric machine in fault or under attack may cause unusual harmonics or energy profile in electrical networks [5].

By analyzing the electrical waveform signals and their root cause, waveform analytics can present utilities with a complete picture of the health and status of their system, both during outages and normal operating conditions. It could also provide a variety of operational benefits to system operators, asset management personnel, and repair crew. Electronic sensors placed on power grids and distribution systems can either measure the electricity properties, such as phasor measurement unit (PMU) sensors [6], [7] or directly record the raw electrical waveform using waveform measurement unit (WMU) [8]–[12], depending on the needed fidelity of monitoring applications. Thanks to developed network connectivity, the streaming monitoring data flow can be obtained and analyzed online and in real-time [13].

The network of the waveform sensors form an Internet of Things (IoT) system [4], [14], where the waveform sensors are viewed as networked IoT sensing devices. Therefore, we can potentially use the information embedded in electrical signals to enable security monitoring, diagnosis, and prognosis in the power networks. The possibility may be well beyond what we can imagine now. It broadly applies to many cyber-physical systems (CPS) and applications, such as power distribution networks, multi-stage manufacturing systems, electric vehicles, and so on [15]–[17]. Cyber attacks towards connected IoT devices trigger anomalies in system statistics, energy consumption, as well as electrical waveforms [4], [14], [18], [19]. Thus, recorded waveform which carries high fidelity current and voltage information should be adequate for cyber attack characterization. Furthermore, the transmission of the high-frequency waveform data is feasible in practice [20]–[22].

Data-driven methods have been widely adopted for event localization in power electronics networks and active distribution systems. Rule-based data-driven analytics [23], signal property-based approach [24], and neural networks (NN) based algorithms, such as autoencoders [25], convolutional neural network (CNN) [26], have been developed. However, NN-based algorithms typically require a large amount of training data to capture the sophisticated features, which cannot be fully simulated or acquired from real applications. Thus, combining the rule-based signal processing methods and machine learning methods could lead to a solution tackling the challenging problem using an affordable data size.

There have been numerous works targeting the event and cyber attack localization problem [1], [2], [27]. Dynamic

Manuscript received XXX, 2021; revised XXX, 2021; accepted XXX, 2021. This work was supported by National Key Research and Development Project under Grants 2018YFC1900800 and 2018YFC1900805, National Science Foundation of China under Grants 61890930-5, 61903010, 62021003 and 62125301, Beijing Outstanding Young Scientist Program under Grant BJJWZYJH01201910005020, and Beijing Natural Science Foundation under Grant KZ202110005009. And this research is also partially supported by the U.S. Department of Energy's Solar Energy Technology Office under award number DE-EE0009026, U. S. National Science Foundation NSF-ECCS-1946057, and Southern Company. (*Corresponding author: Fangyu Li*)

Q. Li, J. Zhang, J. Ye and W. Song are with Center for Cyber-Physical Systems, University of Georgia, Athens, GA 30602, USA (e-mail: qi.li@uga.edu, jinan.zhang@uga.edu, jin.ye@uga.edu, wsong@uga.edu).

J. Zhao is with Department of Electrical and Computer Engineering, University of Connecticut, Storrs, CT 06269 USA (e-mail: junbo@uconn.edu).

F. Li is with Faculty of Information Technology, Beijing Key Laboratory of Computational Intelligence and Intelligent System, Engineering Research Center of Digital Community, Ministry of Education, and Beijing Artificial Intelligence Institute, Beijing University of Technology, Beijing 100124, China. (e-mail: fangyuli2020@gmail.com).

data analytics based localization is always a major branch for the distribution networks [1], DC microgrid [2], islanded microgrid [27]. This paper proposes a new adaptive hierarchical framework for efficient and accurate cyber attack detection and localization by taking advantage of the electrical waveforms (Fig. 1). The proposed approach has a hierarchical architecture that divides the whole network into sub-groups and then locates the cyber attack within one local cluster. Based on a modified unsupervised clustering and an deep learning based anomaly detection method, cyber attacks in the active distribution systems can be adaptively detected and located. The performance of the proposed approach has been tested by multiple cyber attack scenarios in two representative case studies.

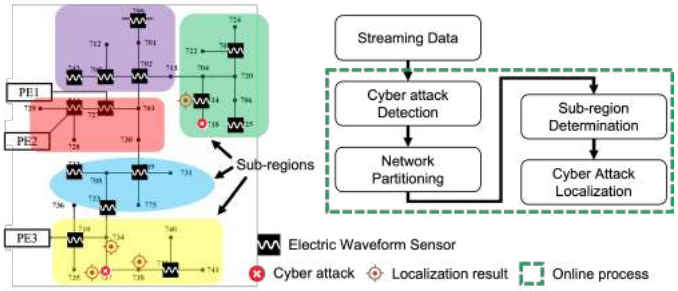

Fig. 1: The proposed adaptive hierarchical online cyber attack localization workflow. The details are discussed in Section III.

Our contributions are summarized as follows:

- We propose an adaptive hierarchical cyber attack detection and localization framework for active distribution systems with DERs using the electrical waveform;
- High fidelity models of DER and cyber attacks are built to analyze the impacts of cyber attacks towards the distribution networks;
- Extensive experiments are utilized to evaluate the proposed approach performances with quantitative analytics;

The remainder of this paper is organized as follows. In Section II, the cyber attack model of active distribution systems is discussed. In Section III, we describe the proposed approaches with the details of each key component, which are cyber attack detection, network partition and cyber attack localization. Experiments and evaluations can be found in Section IV. In the end, a conclusion is drawn in Section V.

II. Cyber Attack Model

Cyber attacks on power systems and smart grids have become more common, especially with the increasing number of power electronics converters. Specifically, PV embedded active distribution system is one of the most representative examples. For smart inverters in the distribution systems, false data integrity (FDI) attack is one of the common cyber-attacks when an enormous amount of DERs are connected to the power system [28], [29]. Besides the high order abnormal harmonics caused by the cyber attacks towards the power electronics devices in the power system, FDI attack could also manipulate the critical threshold in relays [30] and transformers [31] to induce the short circuit faults. In addition, the research on FDI attacks against distribution system SE (DSSE) is an interesting open area. In [32], the vulnerability of distribution system SE (DSSE) to FDI attack was investigated. The work in [33] provides a basis to study the attack behaviors in distribution systems and a theoretical guide to develop protective countermeasures. Authors in [34] attempt to optimize the effectiveness and hiddenness of Moving Target Defense (MTD) while considering voltage stability. MTD is a new technology to defend against the FDI attack on DSSE.

In this paper, to simulate cyber attacks that occurred in the active distribution grid, FDI attack is modeled here, which is assumed to falsify the sensor measurements and degrade controller performance. FDI attack is defined as

$$Y = \alpha\ Y_f + \beta\ Y_0, \tag{1}$$

where Y is the falsified data vector that is eventually used by the controller, Y_0 is the original measurement, Y_f is a fake data vector which can be independent or determined by Y_0, α is a coefficient that determines the weight of the attack vector, β is a coefficient that defines the weight of the measurement.

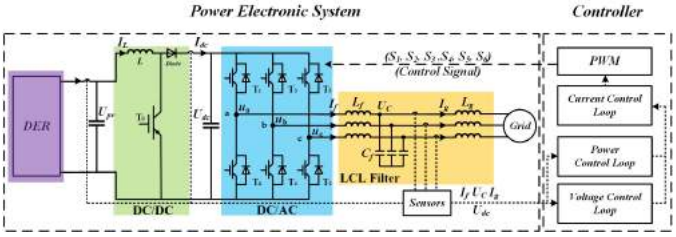

Fig. 2: The adopted cyber attack model of the studied active distribution systems. The vulnerability of the smart inverter due to FDI attacks is shown.

In the PV (photovotaic) converter controller in the Fig. 2, Y_0 is shown as

$$Y_0 = [U_{pv}, I_{pv}, U_{dc}, I_f, U_c, I_g]^T. \tag{2}$$

where U_{pv}, I_{pv} are the PV array voltage and current, respectively. U_{dc} is DC link voltage, I_f is the inverter-side current in LCL filter, U_f is the capacitor voltage in LCL filter, I_g is the grid-side current in LCL filter. As for the phase voltage source inverter (VSI), Y_0 only includes I_f, U_c and I_g. Both Fig. 2 and Fig. A.1 show the vulnerability of the inverter due to FDI attacks. More detailed model of DERs in this paper is illustrated in the Appendix A.

III. Proposed Approach

The workflow of the proposed adaptive hierarchical cyber attack localization approach is shown in Fig. 1. It includes online processing procedures, such as cyber attack detection, network partitioning, sub-region determination, and cyber attack localization. In this section, we introduce the methodologies in detail with thorough discussions. Note that we assume the optimal sensor placement (OSP) has been done offline. The purpose of OSP to achieve the observability of the whole distribution system with the minimum number of waveform sensors [35].

A. Cyber Attack Detection

Distribution power systems typically operate under steady-state. Therefore, the cyber attack can be detected based on the deviation of the monitoring metrics from steady-state, which, in our study, is an anomaly detection problem. For time-series sensor streaming data, statistical analysis is typically used for cyber attack detection [13], [14]. Our previous studies [13], [15] utilizing the data-driven methods have shown remarkable performance regarding the electrical waveform data. By applying the cyber attack detection algorithm on streaming waveform measurement unit (WMU) data, we can determine if there is a cyber attack in real time. In this case, cyber attack detection is treated as a one-class classification problem. A Multi-layer Long Short-Term Memory Network (MLSTM) from our previous work has been applied, which not only remembers sequential information but also carries out a more rigorous screening of time information. So, we can generalize the behavior complexity of the active distribution systems without a huge dataset. Besides, detectors such as CUSUM, DBSCAN, and our MLSTM, are compared.

B. Network Partition based on Modified Spectral Clustering

To efficiently locate the cyber attacks, we propose to first partition the active distribution systems into several sub-regions. It is similar to divide a centralized problem into smaller problems and solving them in a distributed manner. Spectral clustering is a classic unsupervised learning method based on the graph theory to partition a graph into several sub-graphs [36], [37], which is easy to implement and performs well. Therefore it is suitable for the active distribution system partition in our study. We propose a modified spectral clustering to search for the optimal partition results.

Algorithm 1 Modified Spectral Clustering

1: **Input:** Adjacency matrix A, data matrix X and cluster number K.
2: Compute the Affinity matrix S based on the data matrix.
3: Compute the modified Laplacian matrix $\mathcal{L} = (D - S) + \mu(D - A)$.
4: For K clusters, compute the first K eigenvectors $[v_1, v_2, \ldots, v_K]$.
5: Stack the vectors to form a matrix with the vectors as columns.
6: Represent every node by the corresponding row of the stacked matrix, which forms the feature matrix.
7: Use K-means clustering to cluster data samples into K clusters $\{C_1, C_2, \ldots, C_K\}$.

Let $A \in \mathbb{R}^{N\times N}$ be the adjacency matrix of our WMU sensor topology and its entry is defined as

$$A_{ij} = \begin{cases} \frac{1}{Z_{ij}}, & \text{if node } i \text{ and } j \text{ are connected.} \\ 0, & \text{otherwise.} \end{cases} \tag{3}$$

where Z_{ij} is the impedance between vertex i and vertex j. In this case, $A_{ij} = \frac{1}{Z_{ij}}$ if vertex i and vertex j are connected in the original active distribution system topology and $A_{ij} = 0$ if vertex i and vertex j are not connected directly. Let $D = \text{diag}(A\mathbb{1}_n)$ be the diagonal matrix where D_{ii} is the degree d_i of node i, i.e., $d_i = \sum_{j=1}^{N} A_{ij}$. In addition, let $S \in \mathbb{R}^{N\times N}$ be the affinity matrix calculated based on the measurement correlations. This measurement correlation could be customized as long as it could represent the electrical distance among nodes. Since we have considered three-phase unbalance in our models, it should be pointed out that we use the average of three-phase current and voltage to calculate the measurement correlation.

The modified Laplacian matrix $\mathcal{L}$ can be defined as

$$\mathcal{L} = (D - S) + \mu(D - A), \tag{4}$$

where μ is a penalty term, without losing generality, to balance the influences on grid partition result from static topology and dynamic data structure. Then, the eigenstructure of the Laplacian matrix $\mathcal{L}$ is analyzed to decide which cluster the nodes belong to. The details of the modified spectral clustering can be found in Algorithm 1.

C. Cyber Attack Localization within Sub-regions

Combining our proposed cyber attack detection and modified spectral clustering, the cyber attack can be located into a sub-region of the large-scale networks. Furthermore, we need to locate the cyber attack within the sub-regions. Following the assumption that the affected waveform signals show different influences according to the distances between the sensor locations and the cyber attack location, we propose a signal anomaly strength-based approach to detect the exact location of the cyber attack. The location of WMU's placement plays a vital role in better observability and localization of cyber attacks. Note that, in our study, we assume the topology is known beforehand. Comparing the abnormal scales, the relative distances can be determined. Therefore, the relative locations in the topology can be inferred. However, sometimes, this approach may provide a range instead of a node point, which is already an improvement using limited sensors.

The disturbance at the point of impact of stone is stronger, but it fades out soon, and at the other end of the lake, no such disturbance can be visibly detected. Similarly, the WMU can detect the cyber attacks if they are near the cyber attack location, and in some cases, multiple WMU can detect the cyber attacks. Cyber attacks which have a more significant impact will generate obvious signatures and can be detected in multiple WMU. However, some minor cyber attacks or cyber attacks are local, and their signatures are not strong enough to be picked up by WMUs far in the electrical distance in the network. Therefore, we compute statistical parameters and get a normalized score to determine the WMU with the strongest signal for a particular. This method helps extract information based on WMU data.

1) Impact Scores of WMUs: To characterize the pattern of the waveform data, we proposed the following four (4) statistical measures:

- *Standard Deviation* σ: σ is suitable for measuring the data distribution and in our case the disturbance caused by the attack in waveform data. σ can be calculated as:

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(X_i - \mu)^2}, \tag{5}$$

where 'X' is the stream data, 'i' is the index of the stream data window length 'N', and μ is the mean of data window.

- *Range*: Range measures the pattern variation of WMU data during the cyber attack. It can be expressed as:

$$Range = |\max(X_i) - \min(X_i)|, \tag{6}$$

where the data ranges from '$i = 1$' to '$i = N$' and N is the window length.

- *Mean Difference (MD)*: MD is calculated using data points in previous and current windows. MD captures the information on the magnitude shift, and is defined as:

$$MD = |\mu_{\text{previous}} - \mu_{\text{current}}|, \tag{7}$$

where μ_{previous} and μ_{current} are the mean value of the previous and current data windows, respectively.

- *Peak Factor (PF)*: PF measures the severity of the crest of the data during cyber attacks. A WMU close to the cyber attack would have a larger PF than a WMU which is far away from the cyber attack. PF is calculated following:

$$PF = \frac{max(X_i)}{\frac{1}{N}\sum_{i=1}^{N}(X_i)^2}. \tag{8}$$

The nearest WMU from the cyber attack location regarding electrical distance will see more prominent cyber attack signatures. The respective values of the above discussed statistical measures would be higher. However, it is unfeasible to compare the scores of each measure computed above across WMUs. Normalization helps in the identification of prominent WMUs for a particular cyber attack by comparing the single-point scores. In our case, the normalized *impact score* is calculated as:

$$IS = PF \times (\sigma + Range + MD). \tag{9}$$

2) forming subgraph and subgraph scanning: After calculating the normalized impact score, the next step is to select the top WMUs based on the scores. Several WMUs detect specific cyber attacks as their system-level impact is higher. A cyber attack would be seen by multiple WMUs, and a transformer tap change or a load change would be sensed locally by WMUs at those buses, at adjacent buses, or WMUs placed close to the cyber attack bus in terms of electrical distance.

The process of the subgraph scanning and cyber attack localization are explained in Algorithm 2. It takes the clustering result matrix and cyber attack detection result as the inputs. From the cyber attack detection result, the cluster including the cyber attack nodes will be selected. Then, the normalized IS score of each element in the selected cluster will be calculated. Depending on if the cyber attack location is on the WMU bus or not, the output cyber attack location will be the node with the highest IS score or between the first highest IS score node and the second highest IS score node.

Algorithm 2 Subgraph scanning and localization

Input *clustering result matrix*, *cyber attack detection result*.
Output *Subgraph, Cyber Attack location*

1: From the proposed spectral clustering result, select the cluster which comprises the cyber attack nodes based on the detection result.
2: $Subgraph = selected\ cluster$
3: Compute the Normalized Impact Score [Eq. (9)] for each element in subgraph.
4: $CyberAttackLocation = WMU\ with\ highest\ IS$
5: **if** *Cyber attack location is not on the WMU bus* **then**
6: Pick the WMU with 2nd highest IS
7: $CyberAttackLocation$ is in between the 1st highest IS WMU and 2nd highest IS WMU
return $SubGraph$, $CyberAttackLocation$

IV. Experiment

Our design is designed for the cyber attacks towards active distribution systems, while the experiment is evaluated and demonstrated with DERs in the study cases.

A. Simulation Setup

First, an IEEE 37-node distributed grid is built in OPAL-RT. Based on the power grid topology, two PV farms and a VSI based DER are connected to the grid shown in Fig. 3. The smart grid system is connected to the main power grid via node 799, so node 799 can be viewed as a voltage source. The PV farm I (node 727) has a power generation of 390kW; PV farm II (node 710) has a power generation of 120kW; The DER (node 744) has a power generation of 130kW.

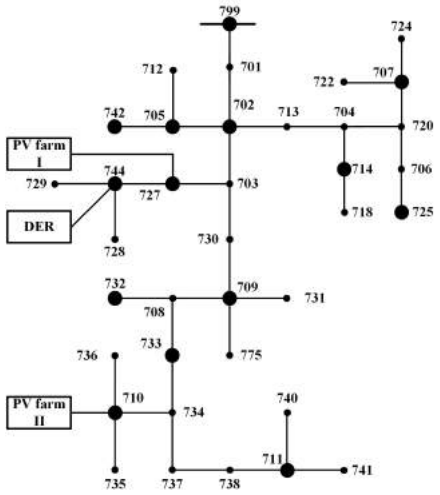

Fig. 3: A smart grid example with solar farms, which is based on the IEEE 37 node model. And the sensor locations from OSP are indicated by the black filled circles.

The FDI attacks modeled in section II are implemented in PV farms and DER. Three FDI attacks, which are shown in Table I, are designed for compromising the converter controller of different DERs. In addition, an FDI induced three-phase

short circuit fault is also simulated to verify the algorithm feasibility.

TABLE I: Details about FDI attacks towards the power grid.

Attack	α	β	Y_f	Target
Case1	$diag[0\ 0\ 0\ -0.9\ -0.9\ -0.9\ 0\ 0\ 0\ 0\ 0\ 0]$	1	Y_0	PV I
Case2	$diag[0.7\ 0.7\ 0.7\ 0.5\ 0.5\ 0.5\ 0.1\ 0.1\ 0.1]$	0	Y_0	DER
Case3	$diag[0\ 0\ 0.7\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]$	1	Y_0	PV II

Using the OSP method [35], the sensor placement results in the IEEE 37-node distribution network model are obtained (Fig. 3), where 14 waveform sensors should be placed at the corresponding nodes to make the system numerically observable. Therefore, we collect 98 (7×14) dimension streaming data, where 3 phase currents, 3 phase voltages, and 1d time stamp are included. To fully observe the power system behaviors, including both normal and abnormal activities, we simulated one (1) minute long data. Because of the 10000 Hz sampling frequency, the data length is 600001, resulting in a data measurement matrix 98×600001 for each case. Thus, efficient data analysis is required to process the extensive amount of data. Figs. 4 and 5 show the examples of the WMU current and voltage data samples in different cases, respectively.

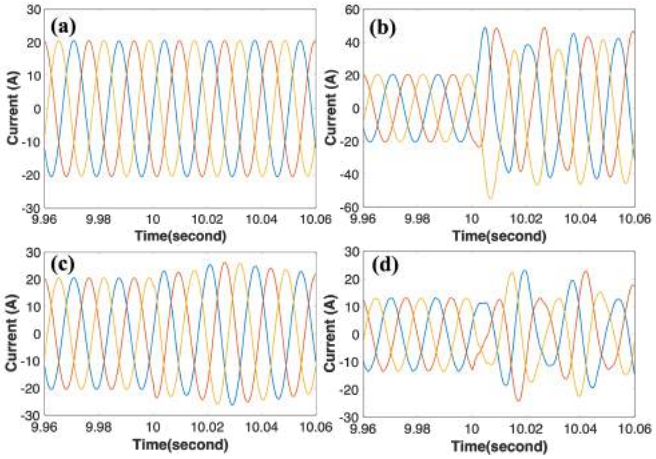

Fig. 4: Current waveform examples captured by WMU sensors: (a) Node 744 under normal case; (b) Node 744 under cyber attack; (c) Node 744 when node 706 is under cyber attack; (d) Node 733 when node 710 is under cyber attack.

B. Cyber Attack Detection

As described in section III-A, our previous MLSTM model is adopted to implement real-time cyber attack detection. We also compare it with linear regression, CUSUM [38], and DBSCAN [39]. The comparison results are shown in Table II. In a quantitative data-driven experiment evaluation, there are four important metrics: true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN). TP denotes the rate of actual attack correctly predicted as an attack, TN denotes the rate of actual normal correctly predicted as normal,

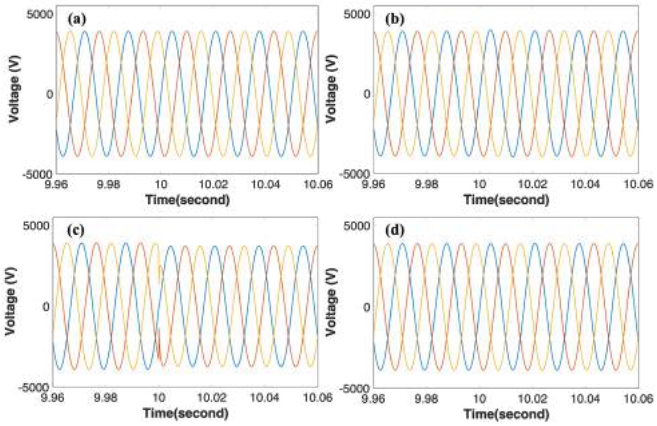

Fig. 5: Corresponding voltage waveforms to the current waveforms shown in Fig. 4 captured by WMU sensors. Note that the waveform distortions are more obvious in the current waveforms.

FP denotes the rate of actual attack is incorrectly predicted as normal, FN denotes the rate of actual normal incorrectly predicted as normal. Precision ($Precision = TP/(TP + FP)$) and recall ($Recall = TP/(TP+FN)$) are used to evaluate the model's performance in a more comprehensive way. Precision shows what proportion of positive identifications was actually correct, which quantifies the number of positive class predictions that actually belong to the positive class. Recall tells what proportion of actual positives was identified correctly, which quantifies the number of positive class predictions made out of all positive examples in the dataset. By combining both Precision and Recall, we could have a more accurate understanding of our model's performance, especially when dealing with an unbalanced dataset.

TABLE II: Performance of different detectors

Methods	Precision	Recall
Linear Regression	0.8803	0.6425
DBSCAN	0.6213	0.5977
CUSUM	0.7296	0.7401
Proposed	**0.9523**	**0.9662**

C. Active Distribution System Partition Results

To compare, we applied both the traditional spectral clustering algorithm and the modified spectral clustering defined in Algorithm 1 to implement the grid partitioning. We demonstrate the power grid partitioning result based on the traditional spectral clustering method in Fig. 6, and the result based on the proposed method in Fig. 7. Our proposed method brings in a more condensed and connected clustering result, making more sense in the sub-region partitioning.

Two cases are discussed here. The first case is that a cyber attack towards the PV farm inverter (node 727) happens. Figs. 8 and 9 show the network partitioning results based on the traditional spectral clustering and the proposed modified spectral clustering method, respectively. Although most nodes have the same clustering results, some nodes are showing

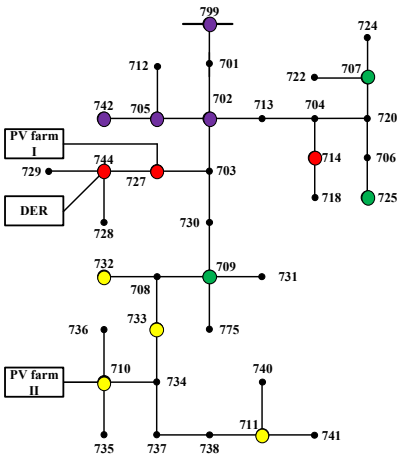

Fig. 6: Power grid partitioning result based on the traditional spectral clustering method in the IEEE 37-node model. Clustered grid nodes are in different colors.

different output labels, such as nodes 702 and 732. The clustering results in Fig. 8 has some problems, such as node 742, which should belong to the same cluster as nodes 705 and 702 because they were clustered together in the normal case shown in Fig. 7 and the cyber attack does not happen near this sub-region. The second case is that an FDI induced three-phase ground fault (short circuit) at node 706.

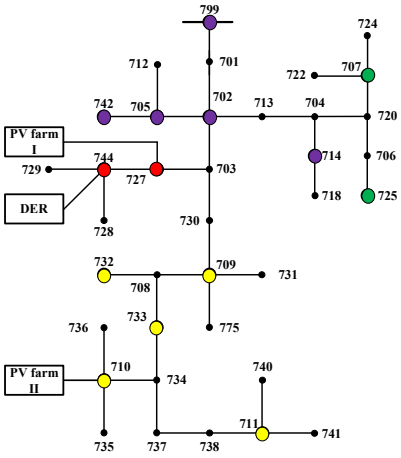

Fig. 7: Power grid partitioning result based on the modified spectral clustering method in the IEEE 37-node model. Clustered grid nodes are in different colors.

Fig. 10 demonstrates the dynamic grid partitioning via traditional spectral clustering, while the proposed modified spectral clustering result is shown in Fig. 11. Intuitively speaking, the modified spectral clustering generates a better result, as the nodes belonging to the same clusters are also geographically located in the same sub-regions. In contrast, some node clustering results in Fig. 10 do not entirely make sense.

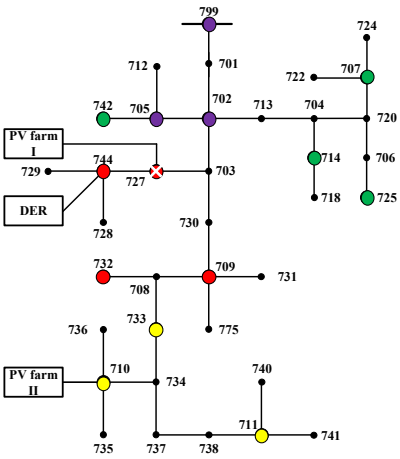

Fig. 8: Network partitioning result based on the traditional spectral clustering when a FDI attack occurs at node 727.

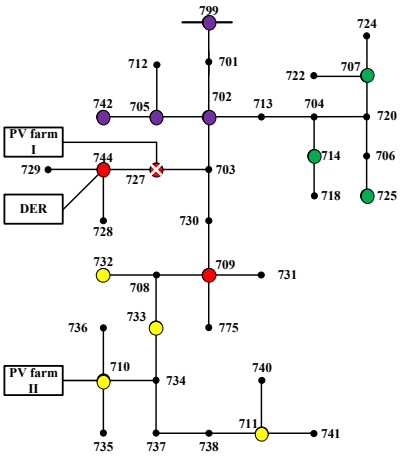

Fig. 9: Network partitioning result based on the proposed clustering method when a FDI attack occurs at node 727.

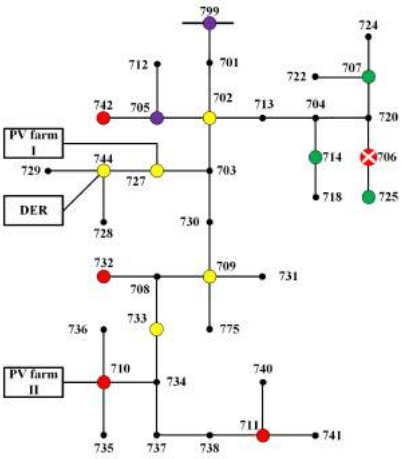

Fig. 10: Network partitioning result based on the traditional spectral clustering when a FDI attack occurs at node 706.

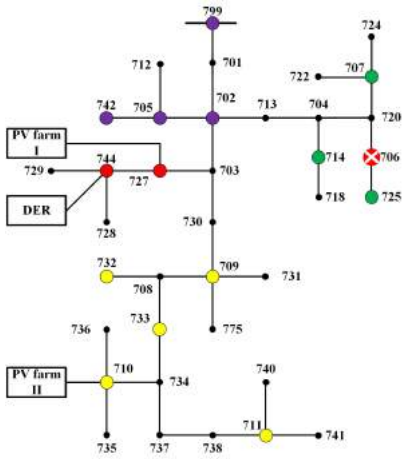

Fig. 11: Network partitioning result based on the proposed modified spectral clustering when a FDI attack occurs at node 706.

To quantitatively analyze the grid partitioning results, we employ the Silhouette score [40] as the index to evaluate the performance of the clustering results. In general, a higher Silhouette value indicates a closer electrical connection inside the sub-region and a looser connection among various sub-regions. The results of the average Silhouette scores of three different clustering methods in two cases are shown in Table. III.

TABLE III: Silhouette score table for IEEE 37-node model

Cases	Methods	Average Silhouette score
Cyber attack	proposed method	**0.8176**
	spectral clustering	0.7611
	Kmeans	0.5707
Ground fault	proposed method	**0.8056**
	spectral clustering	0.7678
	Kmeans	0.7822

We can observe that in both cases, the average Silhouette scores of the proposed modified spectral clustering results are generally higher than the other ways. A higher average Silhouette score indicates that our proposed approach obtains a superior supervised clustering result in terms of the correlation or inner distance. Thus, in both qualitative and quantitative analysis, our proposed approach achieves better results.

D. Cyber Attack Location in the Sub-regions

After clustering nodes into different groups, a more accurate cyber attack location should be estimated. To confirm the cyber attack location, our proposed subgraph scanning and localization algorithm is conducted, whose detail is explained in Algorithm 2. The statistical IS (impact score) of every potential cyber attack location would be calculated, and the node getting highest IS score would be considered as the cyber attack location or the place nearest to the cyber attack location. Taking the FDI attack case at node 727 (Fig. 9) and fault case at node 706 (Fig. 11) as the examples, we calculate the IS score to determine the cyber attack location.

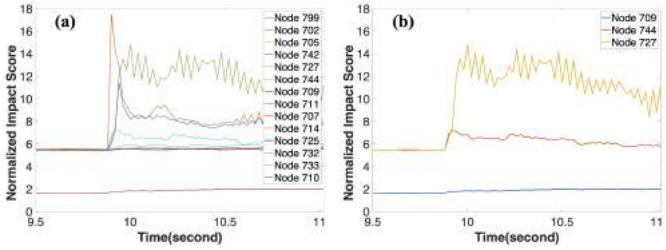

Fig. 12: IS scores for attack on node 727: (a) the whole topology and (b) the subgraph. In both figures, node 727 obviously has the highest IS.

For the FDI attack case, combined with detection result and clustering results, we located the target locations to node 709, 744, 727 as shown Fig. 9. There IS results are shown in the right-side figure in Fig. 12, which shows that node 727's IS is the highest when the attack is happening, indicating the cyber attack should be located in there, and it is actually correct. The left figure shows the IS scores for all the nodes in our power network. Among all the nodes, the node 727's IS is still the highest. It could capture some global topology information but not exactly. Moreover, calculating global IS would cost much more time than just calculating the nodes in the sub-graph.

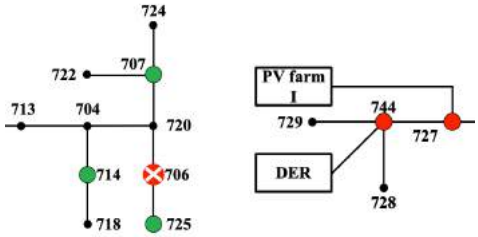

Fig. 13: Sub-regions (a) with the cyber attack and (b) without the cyber attack in Fig. 11.

For the cyber attack case at node 706, combined with detection result and clustering results, we located the target locations to node 707, 714, 725 as shown Fig. 11. Fig. 13 shows two sub-regions with cyber attack (Fig. 13(a)) and without cyber attack (Fig. 13(b)).

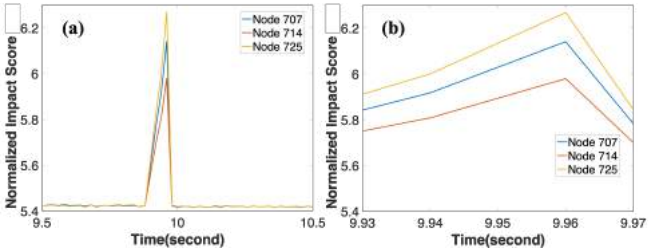

Fig. 14: (a) IS score for FDI induced three phase short circuit fault on node 706. (b) zoom in version of (a). From both figures, node 725 obviously has the highest IS, which is nearest to the cyber attack location.

Their IS results are shown in Fig. 14. It shows that node 725's IS is the highest when the fault is happening, but in

this case, it's not the same node; otherwise, the difference between each node should be more significant.Therefore, the cyber attack location should be node 706, which is correct.

We evaluate our localization performance by comparing with the NS (Normalized Score) in the reference [41], which is calculated to locate the cyber attack location in the network using micro-PMU data. Fig. 15 shows the NS results for the nodes of the subgraph in both FDI attack cases. From the figure, we can see that the NS score works well in the ground fault case. However, for the attack on node 727, the result leads us to the wrong location. The NS scores of Node 744 and 727 are higher than the cyber attack location node 725, and they are not distinguishable, which means ours IS score is more robust in terms of the waveform data.

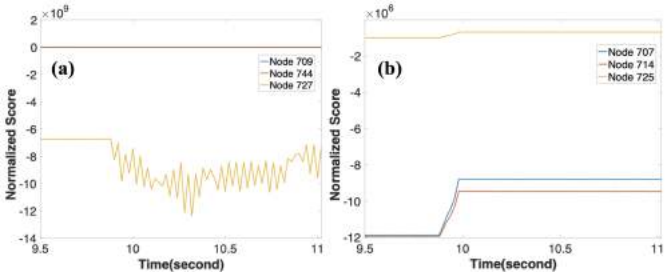

Fig. 15: NS score results: (a) FDI attack case and (b) FDI attack induced fault case.

TABLE IV: Performance with different levels of Gaussian White Noise (cyber attack on the node 744).

	SNR level				
	20dB	15dB	10dB	5dB	0dB
Detection accuracy	100%	100%	90%	70%	55%
Silhouette score	0.7624	0.7601	0.6912	0.6110	0.5411
Localization accuracy	100%	100%	95%	85%	70%

TABLE V: Performance with different levels of Laplace Noise (cyber attack on the node 744).

	SNR level				
	20dB	15dB	10dB	5dB	0dB
Detection accuracy	100%	100%	90%	68%	56%
Silhouette score	0.7615	0.7603	0.6933	0.6102	0.5451
Localization accuracy	100%	100%	93%	82%	70%

E. Robustness and Sensitivity Analysis

To investigate the robustness and sensitivity of the proposed method against various measurement noises, we add white Gaussian noise to the signal with different Signal Noise Ratios (SNRs). Table IV shows the result of an attack on node 744. To get the detection accuracy and Silhouette score in the table, we conduct 20 times experiments with random noise and calculate the average. For the localization accuracy, we only take account when the subgraph is correctly located. Then calculate the average of 20 times experiments. From the result, our proposed method has great robustness against noise, even doing good when SNR is 5dB. When SNR equals 0dB, the signal is submerged by the noise. Since the measurement noise may not follow Gaussian distribution, we also considered adding Laplace noise ($\mu = 0$ and $b = 1$) to the signal. Compared with normal distribution, the Laplace distribution has more flatten or long tails data, which means it has bigger variance. The result is shown in Table V. From the result, we can tell there is no significant difference between Laplace noise and Gaussion noise. Both of them perform well until the signal is almost overwhelmed by noise. It shows that our method captures the characteristics of the sequential data as a whole, which makes it of good robustness.

F. Performance in a Larger-Scale System

To show the scalability of the proposed method, we test the proposed method on the widely used IEEE 123-bus distribution system (Fig. 16), which contains the distribution lines and loads in single-phase, two-phase, and three-phase [42]. To guarantee the observability, WMU sensors are installed on 51 buses which is 41.5% of the total amount (details can be found in Table VI).

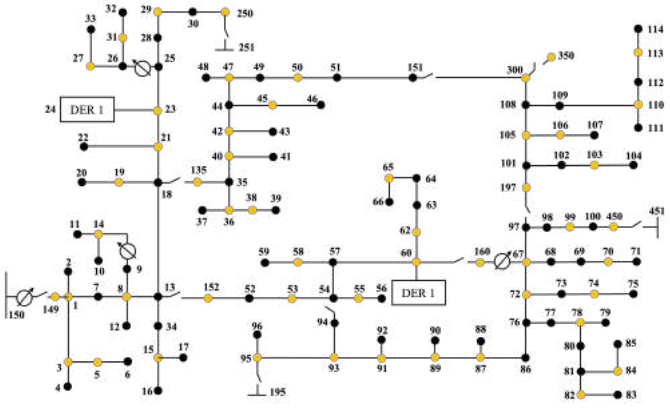

Fig. 16: IEEE 123-bus distribution system. The WMU sensors are marked in yellow.

Following the same setup of the previous IEEE 37-node distributed grid experiment, the IEEE 123-bus system is built in OPAL-RT as well. Three FDI attacks against DER1 and DER2 have been modeled. Figs. 17 and 18 illustrate the partition results when an FDI-induced three-phase ground short circuit fault happens for traditional spectral clustering and our proposed method, respectively. The quantitative results for all cases are shown in Table VII. The proposed approach not only works in this larger grid, but also generates superior results compared to other methods.

TABLE VI: WMU sensors in IEEE 123-BUS system

WMU Sensors Installed Bus	Total No.	Percentage
1, 3, 5, 8, 14, 15, 19, 21, 23, 27, 29, 31, 36, 38, 40, 42, 45, 47, 50, 53, 55, 58, 60, 62, 65, 67, 70, 72, 74, 78, 82, 84, 87, 89, 91, 93, 95, 99, 103, 105, 106, 110, 113, 135, 149, 152, 160, 197, 250, 300, 450	51	41.5%

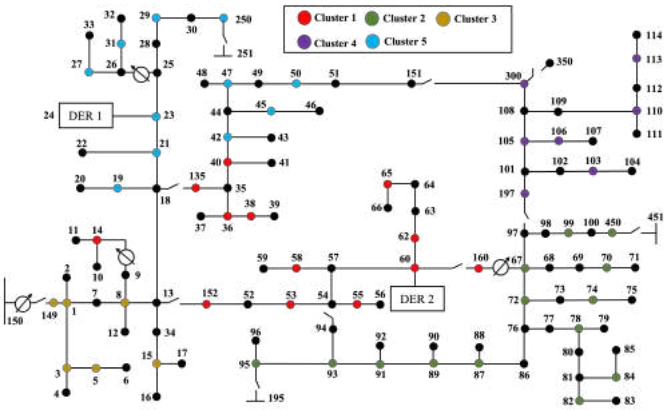

Fig. 17: Power grid partitioning result based on the proposed spectral clustering method in the IEEE 123-bus model. Clustered grid nodes are in different colors.

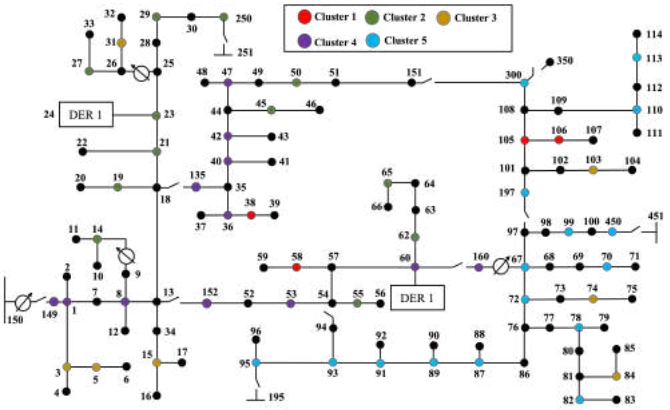

Fig. 18: Power grid partitioning result based on the traditional spectral clustering method in the IEEE 123-bus model. Clustered grid nodes are in different colors.

TABLE VII: Silhouette score table for IEEE 123-bus model

Cases	Methods	Average Silhouette score
FDI attack #1	proposed method	**0.7689**
	spectral clustering	0.6529
	Kmeans	0.5322
FDI attack #2	proposed method	**0.7815**
	spectral clustering	0.5923
	Kmeans	0.5328
FDI-induced fault	proposed method	**0.7615**
	spectral clustering	0.5119
	Kmeans	0.5262

G. Approach Feasibility Discussion

The voltage and current waveform measurements in our study are provided by WMUs (Section. III-A). Such emerging sensors are well-suited to study transient events in power distribution systems [43]. Till now, WMU has been adopted in a few applications, such as harmonic addition and cancellation in transformers [8], sub-synchronous resonance analysis [12], and power quality event localization [44]. Typically, a WMU can report 256 readings per cycle [45]. To support synchronized measurements at a such high rate, WMUs have a time accuracy of 1 μ second [45]. In our IEEE 123-bus study case, the sampling rate is 5000 Hz, namely around 83 readings per cycle, which means the measurement provided by a typical WMU is more than enough to locate nodes under attack.

V. Conclusion

In this paper, we proposed an adaptive hierarchical cyber attack localization approach for active distribution systems. Electric waveform signals obtained by WMU sensors are used to capture the abnormal features, which would be otherwise ignored. To improve the efficiency, we propose a modified spectral clustering method to first partition the whole large network into smaller 'coarse' sub-regions. Next, the accurate 'fine' cyber attack location can be determined by calculating and analyzing Impact Score of each sensor in the potential sub-region. Furthermore, we compare our method with other methods in each step in cyber attack detection, sub-graph clustering, and localization, respectively. The results from two representative distribution grids show that our method shows promising performances.

Appendix A
Modeling Distributed Energy Resources

With more and more DERs integrated into power system, a growing number of security problems are being exposed constantly. Also, the cyber-phyiscal security becomes priority especially considering the evolution of smart inverters in DERs. Here, FDI attacks on PV converter and voltage source inverter are modeled.

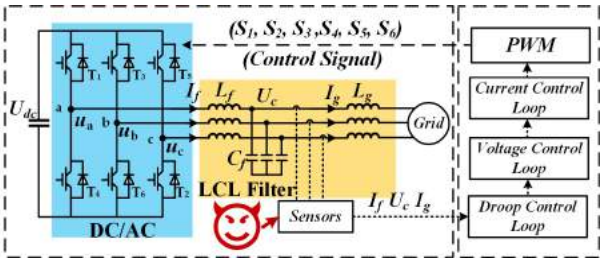

Fig. A.1: Voltage source inverter (VSI) DER model.

Two-stage two-level PV Converter Model

As shown in the Fig. 2, two-stage PV converters are constructed. The first stage includes PV array and DC/DC converter. The PV array voltage U_{pv} and current I_{pv} are the input of DC/DC controller. The MPPT algorithm is applied in DC/DC controller so that PV array generates maximum power to inverter. And the second stage comprises DC/AC inverter and LCL filter. In the DC/AC controller, voltage control loop is used to maintain DC link voltage and generate the current reference I^*_{fd} for the current control loop. The reactive power control loop is built in the controller and determines the I_{fq}. The current loop can be expressed as,

$$\begin{aligned} U^*_{id} &= k_p(I^*_{fd} - I_{fd}) + \frac{k_i(I^*_{fd} - I_{fd})}{s} - \omega L_f I_{fq}, \\ U^*_{iq} &= k_p(I^*_{fd} - I_{fd}) + \frac{k_i(I^*_{fd} - I_{fd})}{s} + \omega L_f I_{fd}, \end{aligned} \tag{A.1}$$

where, $I_{fd,q}$ is inverter side current in the LCL filter, and L_f is the inductance in LCL filter, k_p, k_i are the PI parameters, $U^*_{id,q}$ is the control signal to PWM. The inverter and LCL filter can be modeled as follow,

$$\begin{aligned}
\dot{I_{fd}} &= \frac{1}{L_f}(U_{id} - U_{cd}) + \omega I_{fq}, \\
\dot{I_{fq}} &= \frac{1}{L_f}(U_{iq} - U_{cq}) - \omega I_{fd}, \\
\dot{U_{cd}} &= \frac{1}{C_f}(I_{fd} - I_{gd}) + \omega U_{cq}, \\
\dot{U_{cq}} &= \frac{1}{C_f}(I_{fq} - I_{gq}) - \omega U_{cd}, \\
\dot{I_{gd}} &= \frac{1}{L_g}(U_{cd} - U_{gd}) + \omega I_{gq}, \\
\dot{I_{gq}} &= \frac{1}{L_g}(U_{cq} - U_{gq}) - \omega I_{gd}.
\end{aligned} \tag{A.2}$$

Model of DER Based on Voltage Source Inverter (VSI)

Besides the PV farm, some DERs do not only offer power to the grid but also maintain stability of frequency and voltage. As shown in Fig. A.1, a DER model based on voltage source inverter is built. DC capacitor voltage represents the renewable energy, e.g. wind turbine, battery, etc. The droop control loop is constructed in the controller, which can be expressed as,

$$\begin{aligned}
&\omega = \omega_n - m_p P, \\
&\theta = \omega_n t - \int m_p P dt, \\
&v^*_d = V_n - n_q Q, v^*_q = 0,
\end{aligned} \tag{A.3}$$

where ω_n is the rated frequency, m_p is active power droop coefficient, n_q is active power droop coefficient, P and Q are power reference. Also, the voltage and current control loop is modeled in the controller. Both of two control loop is achieved with a standard PI controller. The current control loop in the VSI is same as in the PV converter. Thus, the model of voltage control loop is only introduced as follow,

$$\begin{aligned}
I^*_{fd} &= k_{pv}(U^*_{cd} - U_{cd}) + \frac{k_{iv}(U^*_{cd} - U_{cd})}{s} - \omega C_f U_{cq}, \\
I^*_{fq} &= k_{pv}(U^*_{cd} - U_{cd}) + \frac{k_{iv}(U^*_{cd} - U_{cd})}{s} + \omega C_f U_{cd},
\end{aligned} \tag{A.4}$$

where, $I^*_{fd,q}$ is current reference for current control loop, and C_f is the capacitor in LCL filter, k_{pv}, k_{iv} are the PI parameters, $U^*_{cd,q}$ is voltage reference for voltage control loop, $U_{cd,q}$ is the capacitor voltage in d,q framework.

REFERENCES

[1] I. Džafić, R. A. Jabr, S. Henselmeyer, and T. onlagić, "Fault location in distribution networks through graph marking," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 1345–1353, 2016.

[2] R. Bhargav, B. R. Bhalja, and C. P. Gupta, "Novel fault detection and localization algorithm for low voltage dc microgrid," *IEEE Transactions on Industrial Informatics*, 2019.

[3] G. Wu, G. Wang, J. Sun, and J. Chen, "Optimal partial feedback attacks in cyber-physical power systems," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3919–3926, 2020.

[4] F. Li, Y. Shi, A. Shinde, J. Ye, and W.-Z. Song, "Enhanced cyber-physical security in internet of things through energy auditing," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5224–5231, 2019.

[5] A. J. Wilson, D. R. Reising, R. W. Hay, R. C. Johnson, A. A. Karrar, and T. D. Loveless, "Automated identification of electrical disturbance waveforms within an operational smart power grid," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 4380–4389, 2020.

[6] P. Dutta, A. Esmaeilian, and M. Kezunovic, "Transmission-line fault analysis using synchronized sampling," *IEEE transactions on power delivery*, vol. 29, no. 2, pp. 942–950, 2014.

[7] I. Sadeghkhani, M. E. H. Golshan, A. Mehrizi-Sani, J. M. Guerrero, and A. Ketabi, "Transient monitoring function–based fault detection for inverter-interfaced microgrids," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 2097–2107, 2016.

[8] A. F. Bastos, S. Santoso, W. Freitas, and W. Xu, "Synchrowaveform measurement units and applications," in *2019 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2019, pp. 1–5.

[9] Schweitzer Engineering Laboratories, Pullman, WA, USA., "SEL-T400L Time Domain Line Protection," https://selinc.com/ products/T400L/, Last Access: July 31, 2020.

[10] Candura instruments, Oakville, ON, Canada., "iPSR intelligent Power System Recorder," https://www.candura.com/ products/ipsr.html, Last Access: July 31, 2020.

[11] D. Borkowski, A. Wetula, and A. Bień, "Contactless measurement of substation busbars voltages and waveforms reconstruction using electric field sensors and artificial neural network," *IEEE Transactions on Smart Grid*, vol. 6, no. 3, pp. 1560–1569, 2014.

[12] B. Gao, R. Torquato, W. Xu, and W. Freitas, "Waveform-based method for fast and accurate identification of subsynchronous resonance events," *IEEE Transactions on Power Systems*, vol. 34, no. 5, pp. 3626–3636, 2019.

[13] F. Li, R. Xie, Z. Wang, L. Guo, J. Ye, P. Ma, and W. Song, "Online distributed iot security monitoring with multidimensional streaming big data," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4387–4394, 2020.

[14] F. Li, A. Shinde, Y. Shi, J. Ye, X.-Y. Li, and W.-Z. Song, "System statistics learning-based iot security: Feasibility and suitability," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6396–6403, 2019.

[15] F. Li, Q. Li, J. Zhang, J. Kou, J. Ye, W. Song, and H. A. Mantooth, "Detection and diagnosis of data integrity attacks in solar farms based on multilayer long short-term memory network," *IEEE Transactions on Power Electronics*, vol. 36, no. 3, pp. 2495–2498, 2021.

[16] A. Wang and J. Shi, "Holistic modeling and analysis of multistage manufacturing processes with sparse effective inputs and mixed profile outputs," *IISE Transactions*, vol. 53, no. 5, pp. 582–596, 2021.

[17] J. Ye, L. Guo, B. Yang, F. Li, L. Du, L. Guan, and W. Song, "Cyber–physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 4, pp. 4639–4657, 2021.

[18] F. Li, R. Xie, B. Yang, L. Guo, P. Ma, J. Shi, J. Ye, and W. Song, "Detection and identification of cyber and physical attacks on distribution power grids with pvs: An online high-dimensional data-driven approach," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, Early Access.

[19] J. Zhang, S. Sahoo, J. C.-H. Peng, and F. G. Blaabjerg, "Mitigating concurrent false data injection attacks in cooperative dc microgrids," *IEEE Transactions on Power Electronics*, 2021, early access.

[20] M. P. Tcheou, L. Lovisolo, M. V. Ribeiro, E. A. Da Silva, M. A. Rodrigues, J. M. Romano, and P. S. Diniz, "The compression of electric signal waveforms for smart grids: State of the art and future trends," *IEEE Transactions on Smart Grid*, vol. 5, no. 1, pp. 291–302, 2013.

[21] Y.-C. Chang and T.-C. Huang, "An interactive smart grid communication approach for big data traffic," *Computers & Electrical Engineering*, vol. 67, pp. 170–181, 2018.

[22] H. Maaß, H. K. Cakmak, F. Bach, R. Mikut, A. Harrabi, W. Süß, W. Jakob, K.-U. Stucky, U. G. Kühnapfel, and V. Hagenmeyer, "Data processing of high-rate low-voltage distribution grid recordings for smart grid monitoring and analysis," *EURASIP Journal on Advances in Signal Processing*, vol. 2015, no. 1, pp. 1–21, 2015.

[23] X. Liang, S. A. Wallace, and D. Nguyen, "Rule-based data-driven analytics for wide-area fault detection using synchrophasor data," *IEEE Transactions on Industry Applications*, vol. 53, no. 3, pp. 1789–1798, 2016.

[24] B. Wang, H. Wang, L. Zhang, D. Zhu, D. Lin, and S. Wan, "A data-driven method to detect and localize the single-phase grounding fault in distribution network based on synchronized phasor measurement," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, p. 195, 2019.

[25] I. Niazazari and H. Livani, "A pmu-data-driven disruptive event classification in distribution systems," *Electric Power Systems Research*, vol. 157, pp. 251–260, 2018.
[26] I. Niazazari, R. J. Hamidi, H. Livani, and R. Arghandeh, "Cause identification of electromagnetic transient events using spatiotemporal feature learning," *International Journal of Electrical Power & Energy Systems*, vol. 123, p. 106255, 2020.
[27] S. F. Zarei, H. Mokhtari, and F. Blaabjerg, "Fault detection and protection strategy for islanded inverter-based microgrids," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 2019.
[28] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505–2516, 2017.
[29] S. Wang, S. Bi, and Y.-J. A. Zhang, "Locational detection of the false data injection attack in a smart grid: A multilabel classification approach," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8218–8227, 2020.
[30] B. R. Amin, S. Taghizadeh, M. S. Rahman, M. J. Hossain, V. Varadharajan, and Z. Chen, "Cyber attacks in smart grid–dynamic impacts, analyses and recommendations," *IET Cyber-Physical Systems: Theory & Applications*, vol. 5, no. 4, pp. 321–329, 2020.
[31] M. Stănculescu, S. Deleanu, P. C. Andrei, and H. Andrei, "A case study of an industrial power plant under cyberattack: Simulation and analysis," *Energies*, vol. 14, no. 9, p. 2568, 2021.
[32] P. Zhuang, R. Deng, and H. Liang, "False data injection attacks against state estimation in multiphase and unbalanced smart distribution systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6000–6013, 2019.
[33] R. Deng, P. Zhuang, and H. Liang, "False data injection attacks against state estimation in power distribution systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2871–2881, 2018.
[34] M. Liu, C. Zhao, Z. Zhang, R. Deng, and P. Cheng, "Analysis of moving target defense in unbalanced and multiphase distribution systems considering voltage stability," in *2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2021, pp. 207–213.
[35] M. Jamei, R. Ramakrishna, T. Tesfay, R. Gentz, C. Roberts, A. Scaglione, and S. Peisert, "Phasor measurement units optimal placement and performance limits for fault localization," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 1, pp. 180–192, 2020.
[36] J. Shi and J. Malik, "Normalized cuts and image segmentation," *IEEE Transactions on pattern analysis and machine intelligence*, vol. 22, no. 8, pp. 888–905, 2000.
[37] U. Von Luxburg, "A tutorial on spectral clustering," *Statistics and computing*, vol. 17, no. 4, pp. 395–416, 2007.
[38] J. D. Healy, "A note on multivariate cusum procedures," *Technometrics*, vol. 29, no. 4, pp. 409–412, 1987.
[39] E. Schubert, J. Sander, M. Ester, H. P. Kriegel, and X. Xu, "Dbscan revisited, revisited: why and how you should (still) use dbscan," *ACM Transactions on Database Systems (TODS)*, vol. 42, no. 3, pp. 1–21, 2017.
[40] R. Xu and D. Wunsch, "Survey of clustering algorithms," *IEEE Transactions on neural networks*, vol. 16, no. 3, pp. 645–678, 2005.
[41] S. Pandey, A. K. Srivastava, and B. G. Amidan, "A real time event detection, classification and localization using synchrophasor data," *IEEE Transactions on Power Systems*, vol. 35, no. 6, pp. 4421–4431, 2020.
[42] H. Jiang and Y. Zhang, "Short-term distribution system state forecast based on optimal synchrophasor sensor placement and extreme learning machine," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*. IEEE, 2016, pp. 1–5.
[43] M. Izadi and H. Mohsenian-Rad, "Synchronous waveform measurements to locate transient events and incipient faults in power distribution networks," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4295–4307, 2021.
[44] ——, *Event Location Identification in Distribution Networks Using Waveform Measurement Units*. IEEE, 2020.
[45] C. instruments. ipsr intelligent power system recorder. [Online]. Available: https://www.candura.com/ products/ipsr.html

Qi Li received the B.S. degree in Optoelectric Information Science and Engineering from Chongqing University in 2014 and M.S. in Computer Engineering from Chongqing University, Chongqing, China, in 2019. Currently he is pursuing a Ph.D. degree at the University of Georgia, Athens, GA, USA. He is also a Research Assistant at the University of Georgia, USA. His current research focuses on cyber-physical systems and distributed system.

Jinan Zhang received the B.S. degree from North China Electric Power University in 2012 and M.S. in Electrical Engineering from Tianjin University, Tianjin, China, in 2015. Currently he is pursuing a Ph.D. degree with the University of Georgia, Athens, GA, USA. He is also a Research Assistant with the University of Georgia, USA. His current research focuses on security and resilience in power-electronics-based power systems.

Junbo Zhao is an assistant professor of the Department of Electrical and Computer Engineering at the University of Connecticut. He was an assistant professor and research assistant professor at Mississippi State University and Virginia Tech from 2019-2021 and 2018-2019, respectively. He received the Ph.D. degree from Bradley Department of Electrical and Computer Engineering Virginia Tech, in 2018. He did the summer internship at Pacific Northwest National Laboratory in 2017. He is the Principal Investigator for a multitude of projects funded by the National Science Foundation, the Department of Energy, National Laboratories, and Eversource Energy. He is now the chair of IEEE Task Force on Power System Dynamic State and Parameter Estimation and IEEE Task Force on Cyber-Physical Interdependency for Power System Operation and Control, co-chair of the IEEE Working Group on Power System Static and Dynamic State Estimation, the secretary of IEEE PES Bulk Power System Operation Subcommittee and IEEE Task Force on Synchrophasor Applications in Power System Operation and Control. He has published three book chapters and more than 100 peer-reviewed journal and conference papers. He serves as the Associate Editor of IEEE Transactions on Power Systems, IEEE Transactions on Smart Grid, International Journal of Electrical Power Energy Systems, North America Regional Editor of the IET Renewable Power Generation, and subject editor of IET Generation, Transmission Distribution. He has been listed as the 2020 and 2021 World's Top 2% Scientists released by Stanford University in both Single-Year and Career tracks. He is the receipt of the best paper awards of the 2020 and 2021 IEEE PES General Meeting (3 papers), IEEE I&CPS Asia 2021, and the 2020 Journal of Modern Power Systems and Clean Energy, Top 3 Associate Editor award of IEEE Transactions Smart Grid in 2020, the 2020 IEEE PES Chapter Outstanding Engineer Award, and the 2021 IEEE PES Chapter Outstanding Volunteer Award. My research interests are cyber-physical power system modeling, monitoring, uncertainty quantification, learning, dynamics, stability control, and cyber security with DERs.

Jin Ye received the B.S. and M.S. degrees in electrical engineering from Xi'an Jiaotong University, Xi'an, China, in 2008 and 2011, respectively, and the Ph.D. degree in electrical engineering from McMaster University, Hamilton, ON, Canada, in 2014.

She is currently an Assistant Professor of electrical engineering and the Director of the Intelligent Power Electronics and Electric Machines Laboratory, University of Georgia, Athens, GA, USA. Her current research interests include power electronics, electric machines, energy management systems, smart grids, electrified transportation, and cyber-physical systems. Dr. Jin Ye is the General Chair of 2019 IEEE Transportation Electrification Conference and Expo (ITEC), and the Publication Chair and Women in Engineering Chair of 2019 IEEE Energy Conversion Congress and Expo (ECCE). She is an Associate Editor for IEEE TRANSACTIONS ON POWER ELECTRONICS, IEEE OPEN JOURNAL OF POWER ELECTRONICS, IEEE TRANSACTIONS ON TRANSPORTATION ELECTRIFICATION, and IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY.

WenZhan Song received his Ph.D. in Computer Science from Illinois Institute of Technology (2005), B.S. and M.S. degrees from Nanjing University of Science and Technology (1997 and 1999). He is a Chair Professor of Electrical and Computer Engineering in the University of Georgia. Dr. Song's research focuses on cyber-physical systems and their applications in energy, environment, food and health sectors. He received NSF CAREER award in 2010.

Fangyu Li received the Ph.D. in Computational Geophysics from The University of Oklahoma in 2017. His Master (2013) and Bachelor (2009) degrees were both in Electrical Engineering, obtained from Tsinghua University and Beihang University, respectively. From 2017 to 2020, he was a postdoctoral fellow with the College of Engineering, University of Georgia. From 2020 to 2021, he was an assistant professor with the Department of Electrical and Computer Engineering at Kennesaw State University. Dr. Li is currently a full professor and PhD supervisor with the Faculty of Information Technology at Beijing University of Technology. His research interests include complex signal processing, machine learning, deep learning, distributed computing, complex system modeling and monitoring, Internet of things (IoT), and cyber-physical systems (CPS).