**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, N 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 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.

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.