Adaptive Hierarchical Cyber Attack Detection and Localization in Active Distribution Systems

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 subregion.

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.

**EXISTING SYSTEM**

Cyber and physical attacks threaten the security of distribution power grids. The emerging renewable energy sources such as photovoltaics (PVs) introduce new potential vulnerabilities. Based on the electric waveform data measured by waveform sensors in the distribution power networks, in this article, an existing system develops a novel high-dimensional data-driven cyber physical attack detection and identification (HCADI) approach.

First, we analyze the cyber and physical attack impacts (including cyber attacks on the solar inverter causing unusual harmonics) on electric waveforms in the distribution power grids. Then, we construct a high-dimensional streaming data feature matrix based on signal analysis of multiple sensors in the network.

Next, we propose a novel mechanism including leverage score-based attack detection and binary matrix factorization-based attack diagnosis. By leveraging the data structure and binary coding, our HCADI approach does not need the training stage for both detection and the root cause diagnosis, which is needed for machine learning/deep learning-based methods. To the best of our knowledge, it is the first attempt to use raw electrical waveform data to detect and identify the power electronics cyber/physical attacks in distribution power grids with PVs.

**Disadvantages**

* The system is not implemented Network Partition based on Modified Spectral Clustering.
* The system is not implemented Cyber Attack Localization within Sub-regions.

Proposed System

The system proposes 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.

**Advantages**

* In the proposed system, 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.
* To efficiently locate the cyber attacks, the system proposes to first partition the active distribution systems into several subregions.

**SYSTEM REQUIREMENTS**

➢ **H/W System Configuration:-**

➢ Processor - Pentium –IV

➢ RAM - 4 GB (min)

➢ Hard Disk - 20 GB

➢ Key Board - Standard Windows Keyboard

➢ Mouse - Two or Three Button Mouse

➢ Monitor - SVGA

**SOFTWARE REQUIREMENTS:**

* **Operating system :** Windows 7 Ultimate.
* **Coding Language :** Python.
* **Front-End :** Python.
* **Back-End :** Django-ORM
* **Designing :** Html, css, javascript.
* **Data Base :** MySQL (WAMP Server).