Dynamic Graph-Based Anomaly Detection in the Electrical Grid

Shimiao Li\(^1\), Amritanshu Pandey\(^1\), Bryan Hooi\(^2\), Christos Faloutsos\(^1\), Larry Pileggi\(^1\)

\(^1\)Carnegie Mellon University, \(^2\)National University of Singapore

Given sensor readings over time from a power grid, how can we accurately detect when an anomaly occurs? A key part of achieving this goal is to use the network of power grid sensors to quickly detect, in real-time, when any unusual events, whether natural faults or malicious, occur on the power grid. Existing bad-data detectors in the industry lack the sophistication to robustly detect broad types of anomalies, especially those due to emerging cyber-attacks, since they operate on a single measurement snapshot of the grid at a time. New ML methods are more widely applicable, but generally do not consider the impact of topology change on sensor measurements and thus cannot accommodate regular topology adjustments in historical data. Hence, we propose DYNWATCH, a domain knowledge based and topology-aware algorithm for anomaly detection using sensors placed on a dynamic grid. Our approach is accurate, outperforming existing approaches by 20% or more (F-measure) in experiments; and fast, averaging less than 1.7ms per time tick per sensor on a 60K+ branch case using a laptop computer, and scaling linearly with the size of the graph.