Abstract

Power grids are one of the critical infrastructures in modern society. There has been a rise in cyber-attacks against power grids and other industrial networks since the last decade. Substations are a key part of a power grid, which require. We can defend substations individually to secure the power grid. There has been a lack of research in network intrusion detection systems for industrial systems due to a lack of datasets. Additionally, substation topology vary to a large degree along with the substation automation design. This indicates a need for a simulation platform for substation automation capable of simulating attacks. IEC61850 standard and especially GOOSE protocol is widely adapted in substation automation. We develop a simulation platform based on IEC61850, which is capable of co-simulating both electrical and network domain. Our co-simulator can simulate custom electrical and network topology using OMNet++ and Simulink software. We demonstrate the capabilities of the co-simulator using a step-down substation. Multiple scenarios with sequential and simultaneous operations against primary equipment i.e. transformers and switches are demonstrated. Denial of Service and packet spoofing attack along with multiple ways of command and control have been demonstrated. Co-simulator is also capable of simulating various attacks against primary equipment. We demonstrate it by unauthorized tap change in transformers. Specification-based network intrusion detection systems have been proposed using the output of network simulation to detect attacks against the network. This specification can be built dynamically. Network switches are configured to detect spoofing attacks. Denial of Service attacks are detected by statistical anomaly detection. We attempted to use popular machine learning models, e.g. Isolation Forest, Elliptic Envelope, Gaussian Mixture Model and more, but they produced poor performance. The simulation result is mainly intended to be used for research in defending attacks against physical equipment as future work.