Cyber Attack Identification in the Electric Power Grid by Anomaly Detection

Kakar, Devesh (School: Academy of Aerospace and Engineering)

Brunette, Trevor (School: Academy of Aerospace and Engineering)

Reed, Christopher (School: Academy of Aerospace and Engineering)

Power grids are subject to physical and cybersecurity attacks. A way to help mitigate this threat is to reduce response time by analyzing data reported from the power grid to detect inconsistencies that could represent a breach or malfunction within the grid. These potential failures would be reported and then inspected by a cybersecurity technician who would identify a response. To design such a system, a digital model of the power grid was created by programming a configuration structure with the reported values. That data was then analyzed for indications of an outage, malfunction, or potential breach. Utilizing object-oriented programming within Java, a graphical data structure representing the power grid equipment and each of its measurements was made. Then, a program was created to traverse the data structure while analyzing power and voltage data of each node for inconsistencies, with variable thresholds for tolerating errors. Additional programs were developed to emulate cyber attacks and authenticate the aforementioned anomaly detection software. Next, a physical model was made to record data and test the functionality of the program. The model consists of a transmission transformer, two distribution transformers, and consumer loads. Arduino microcontrollers were used with current and voltage sensors were used to measure and relay data from the model to the program. A breadboard and analog adapters were used to connect the voltage and current sensors to the Arduinos. This data is sent to the Java program, analyzed, and displayed on a laptop, showing the status of the grid.