Simulating the effect of cyber attacks on a Power Grid

Introduction:

This project demonstrates the potential impacts that a False Data Injection and IoT attack have on a power grid

Main Goals:

- Successfully converged power grid
- False Data Injection attack targeting transformers
- IoT attack targeting random buses
- Output results from scripts into shell environment
- Grid shell formation

Implementation:

- Python based project
- PandaPower used for power grid creation
- Pandas used to simulate cyber attacks

Challenges:

- Array out of bounds error during False Data Injection simulation
  - Corrected calculation for number of transformers on grid
- Infinite loop in IoT Attack
  - Added a check to see if all parts of the grid had been attacked to exit loop

Overview:

Our project is aiming to show and simulate the potential risks and outcomes of different cyber attacks being exploited on an electrical power grid. Places like the City of Ames could use this information to help make their power grids more secure. These attacks can lead to an attacker to gain access to a workstation and then proceed to manipulate movement of power throughout the power grid. It is important to prepare for these potential threats because serious damages could occur to a city's distribution of power and leave lasting results. Our project is to help show how power grid companies can see results of specific attacks and the outcome that results from these attacks.

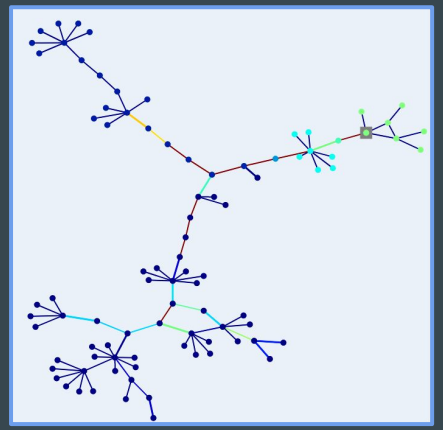
Results:

- Successful visual output of intrusions and affected loads
- Grid creation shell makes power grid for end users

Conclusion:

- Successfully created attack vectors to be used against a simulated grid
- Grid ressemblent of Iowa State's infrastructure
  - Developed a main program to be used for simulation of these attacks
- Grid shell interface
  - Allows for users unfamiliar with power grid components to generate a grid for themselves

IoT Attack



False Data Injection