False Data Injection Attack Model on AC based Hybrid System

Abigail Vincent, Purdue University *NSF Award Number 1600058*

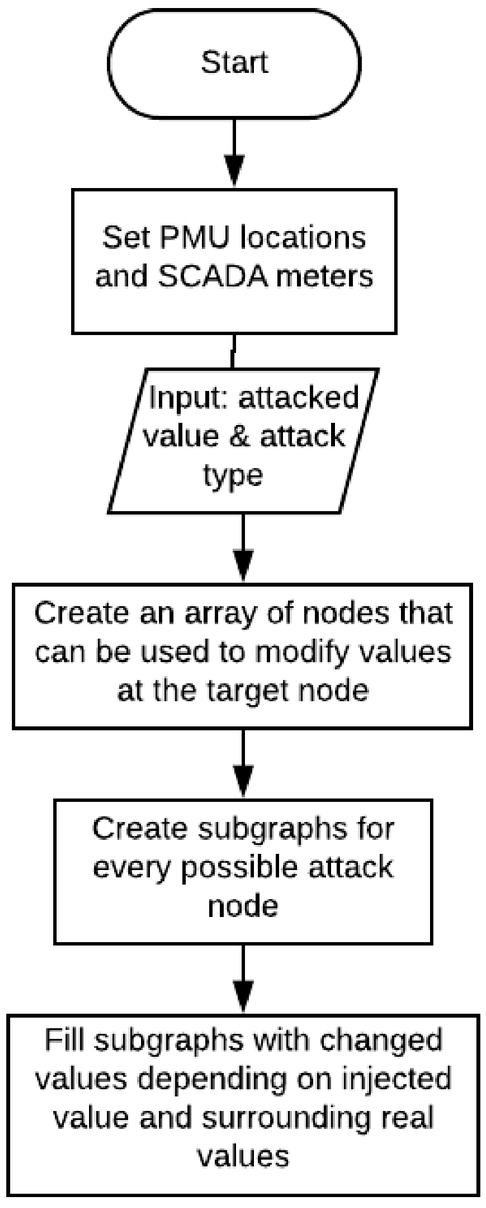
Introduction:

- The power grid is threatened perpetually by cyberattacks. These attacks threaten the livelihood of our modern society as nearly every aspect of our lives relies on technology and in turn electricity.
- One specific type of attack on the power grid is the false data injection attack. These attacks will compromise meters to send readings that mimic realistic data, when the true grid conditions are something else entirely.

Figure 1: An example of a Phasor Measurement Unit that would record data such as voltage, current, and voltage angle with heightened precession.

FIDA Model Development:

- Current research in false data injection attacks have largely been based on SCADA measurements and are tested in DC models. This raises an issue when it comes to plausibility of real-world conditions matching that of prior research.
- Previous AC-based systems were difficult to scale as a result of the computational complexity, but AC based systems are far more realistic than their DC counterparts.
- Additionally, there is now the issue of PMU devices adding previously unconsidered measurements to the grid. This model represents a hybrid system



- **The model that was created is based on a more realistic set of power grid measurements.**
- This model can be used to calculate a false data injection attack, bypassing bad data detection.
- This can be used to test the effects of a false data injection attack in a variety of scenarios.
- This model is specifically being used in testing how the probability of a cascading blackout changes, when a false data injection attack occurs on the power grid.

Solution:

- Created a model based on a **hybrid system** to account for both SCADA measurements and PMU measurement devices
- Select **a single state variable to attack**, modify the surrounding buses to create an “island” of buses and lines that require modification
- The program generates all possible attack regions for a power grid according to the start value and PMU locations
- This new model allows for flexibility in selecting attack regions for testing with false data injection attacks in AC-based systems

Broader Impacts on Society:

- This project allows for further testing of false data injection attacks
- Improved accuracy of testing leads to **more realistic solutions** to counter False Data injection attacks
- Improved security measures against False Data attacks help the security of power systems around the world

Education Impacts:

- Any research conducted about false data injection attacks helps to bring awareness to the true risks that the grid faces daily
- Conducting research in the field of power systems engineering security brings attention to the **vulnerabilities of the power grid** and new devices being implemented

Final Impact:

- The developed attack model can be used with a cascading failure model to quantify the risks of various FDIA on power grids
- The developed model is a fundamental step towards addressing a myriad of questions in power system security