Simulated False Data Injection Attack Outline

SDMAY23-02

Hrijul Balayar, Michael Gierek, Cole Medgaarden, Noah Peake, Conner Spainhower, Jake Stanerson

Foundation

Our simulation was created in order to show realistic results this type of attack would produce if executed on the power grid. A false data injection takes advantage of a system by injecting false and malicious data into a system, causing some sort of harm. We worked to develop a script that would replicate this behavior. Making use of pandas, the underlying library of PandaPower, we are able to manipulate data tables of any grid and change any value of individual parts of the grid; including lines, buses, and substations. For this attack the most realistic point of injection is at substations, as shown in the example below (Ukraine Blackout 2015). By manipulating values of substations of the grid we feel we have replicated the effects of this type of attack.

How it Works

Our attack simulation first takes input for a power grid file to run the attack against. The user is then asked to input the number of attacks they want performed on the grid. In this case it is the number of substations. The script then does error checking to make sure the grid is viable. Next the attack script targets a random substation, by searching for transformers in the grid, and injects a modified voltage value. Substations are only attacked once and the number attacked is based on the user's previous 'attacks' input or until the grid has no more valid targets. Finally, the resulting values are printed in a table and a visual graph is plotted and saved as an html file.

Real World Connection

Ukraine Blackout (2015)
This attack shows that even with certain countermeasures in place, a FDIA is possible on a power grid. In late 2015 attackers were able to cause a blackout in Ukraine's power grid. This attack affected over 200,000 customers. Malware was installed on employee machines. The malware used to complete the attack was able to bypass mechanisms that were in place to detect malicious data; which led to 30 substations being disconnected and the subsequent blackout.