Simulated IoT Device Attack Outline

SDMAY23-02

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

Foundation

This simulation is designed to show the effects of a large-scale IoT device attack and its impact on a power grid. A large-scale IoT attack would cause a noticeable increase in voltage levels than what would be normal in the area it occurred. The script was created using pandas, the underlying library in PandaPower. This attack was designed to mostly target buses within a specified area because it best replicates how an actual large IoT attack would be shown on a grid. We will do that by manipulating the values of the bus to replicate this attack and present the results.

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 to be performed on the grid. The script then does error checking to make sure the grid is viable. Next, the attack script randomly picks a bus to create a target area. The targeted bus and those around it are then manipulated to represent an attack. Finally, the resulting values are printed in a table, and a visual graph is plotted and saved as an HTML file.

Real World Connection

Unsecured University IoT (2017)
This example is of an unknown university where the network was overrun with Domain Name Service (DNS) queries for seafood eateries, as given in Verizon's Data Breach Digest 2017 report. Although it appeared to be a student joke, 5,000 IoT devices, including vending machines and lighting systems, were used in the outside hack. A brute force attack was used to carry out the hack, taking advantage of the university's network's vulnerability to malware deployment.