A Learning Testbed for False Data Injection Attacks

Filip Natvig
Dept. of Electrical Engineering
Uppsala University
Uppsala, Sweden
filip.natvig@angstrom.uu.se

Göran N. Ericsson
Dept. of Electrical Engineering
Uppsala University
Uppsala, Sweden
goran.n.ericsson@uu.se

The power industry faces heightened cybersecurity threats due to increased global connectivity. To protect essential societal functions, safeguarding such critical infrastructures is crucial, necessitating proactive measures to fortify the cybersecurity of electrical power systems. The Ukrainian electric power blackout in December 2015, which affected approximately 225,000 customers, is a stark reminder of the need for defence strategies against one type of cyberattack called false data injection attacks (FDIAs). In recent years, this type of attack has gained some attention among researchers in power system cybersecurity. As a result, numerous testbeds already exist for experimenting with FDIAs and different defence strategies. Nevertheless, they all cater to the same audience: seasoned researchers well-versed in the intricate workings of the hardware and software systems involved in power system control. This uniformity may pose challenges, as it can result in a steep learning curve for new students in power system cybersecurity.

To solve this issue, we have developed a software-based learning tool for introducing power system cybersecurity to a broader crowd and, by extension, fostering research in the field. Specifically, this tool is purposed to enable non-computer-familiar users (particularly power engineering students) to experiment with FDIAs. To address the necessities of this group, we recognize the importance of an intuitive graphical user interface (GUI), allowing the user to run the application without using a command line interface. In addition to making the application more suitable for non-computer-familiar users, we hope this feature will make it more game-like and, thus, more appealing to students.

The current version of the application enables users to simulate the stationary behaviour of an IEEE test system, customize FDIAs to target individual buses, and closely monitor the system's estimated voltage levels through the intuitive GUI. In addition, we have incorporated features that allow users to monitor individual buses closely. However, the application is still in its early stages, and we have several ideas for further enhancements, e.g., by incorporating more advanced attack-customization options, such as the ability to target multiple buses simultaneously. Moreover, from a pedagogical standpoint, the application would benefit from additional functionalities to experiment with detection algorithms. Even though we are actively working on turning these visions into reality, we are embracing help from the community. For this reason, we have open-sourced the project.