In the power grid, control decisions and subsequent actions that directly impact the operation of the power grid are made based on estimation data obtained from the state estimator. A class of cyber-attacks called False Data Injection (FDI) attacks that target measurement data used for state estimation in the power grid are currently under study by the research community. These attacks modify sensor readings obtained from measuring equipment with the aim of misleading the control center into taking ill-advised response action. It has been shown that an attacker with knowledge of the network topology can craft an attack that bypasses existing bad data detection schemes (largely based on residual generation) employed in the power grid.

We propose a multi-agent system that detects FDI attacks targeting state estimation in power grids. The multi-agent system is composed of soft- ware implemented agents created for each substation. The software based agents partition the power network into virtual sub-grids comprising adjacent substations connected by transmission lines and perform state estimation at each of these virtual sub-grids. Off-the- shelf computing and communication infrastructure is deployed in substations providing the software-based agents a means to communicate with each other. The agents facilitate exchange of meter readings among substations that are included in each sub-grid. We demonstrate that the information exchanged among substations, even untrusted, enables agents cooperatively detect disparities between local state variables at the substation and global state variables computed by the state estimator. In the absence of FDI attacks, state estimation results at each sub-grid are identical to state estimation results for the whole grid. However, in the presence of FDI attacks compromised measurements can bypass bad data detection during state estimation for the whole grid. The virtual sub-grids and the main power grid have different topologies such that a successful FDI attack would have to evade bad data detection for the main grid and also for each of the virtual sub-grids making it extremely difficult for a false data injection attack to evade detection in a smart grid equipped with the multi-agent system proposed.

To evaluate the proposed strategy for FDI detection, we conduct experiments with the IEEE 9-bus, 14-bus and 30- bus power system benchmarks using MATPOWER, an open source MATLAB toolbox. For each system, we generate 1000 attack cases that can bypass BDD schemes during state estimation for the whole grid. Then, we deploy agents that construct sub-grids at each substation in the power system and use state estimation at each sub-grid to analyze all FDI cases. In our experiments, we can detect all FDI attack cases with at least one agent.