Research Summary v2

Smart grids use two-way communication and automated load control to help resolve issues with the complexity, demand, and reliability in the current system.

With these additional functionalities, robustness of the overall system has increased. This robustness causes cyber attacks to be difficult to carry out, particularly with the goal of mass takedown of the overall system.

As a result of this, most of the research that has been done to look into vulnerabilities is theoretical. Some of these examples include manipulation of the loads across the network, maximizing node failure, or maximizing the results of cascading failures.

1. One potential avenue that has been explored to try and find vulnerabilities in smart grid systems involves the use of price modification attacks. These attacks cause the load profiles in the system to be altered significantly enough to cause large-scale changes to the load in the overall system. With enough change, failures can start occurring due to the extreme changes in individual loads.

2. Another approach to finding potential weaknesses involves identying critical nodes within the system. Specifically, which nodes are most likely to cause the most nodes to fail as part of a cascading failure. The goal is to determine which nodes would cause the greatest effects if they were to be taken down, generally in smaller numbers.

3. A third possibility to address smart grid robustness details a plan that focuses on both the structural and operative components of the system. Whereas most theories look for attack points in the structure and makeup of the grid, there are relatively few studies that look towards the distribution aspect. When both vectors are targeted simultaneously, there is greater potential to cause large-scale cascading failures across the grid. This can result in more total node failures compared to some of the other theories that do not target both the structural and operative components.