Title: Malware in Smart Grids

Abstract:

With the advancement in communication technology of smart grid, cyber-attacks are becoming the serious threat. Specifically, the vulnerabilities created due to the successful malware installation in smart grid is a very serious concern since it can be exploited to disable the system along with taking control or damaging the critical infrastructure permanently. The main idea behind this thesis is to explore the malware issue in the remedial action scheme (RAS), widely used for wide area protection, of smart grid. The main contribution of the work is divided into two major parts.

In the first part, we modelled the stealthy coordinated cyber-attack with a malware at its core. The purpose of this attack is to damage the grid without getting detected by legitimate users. The attack uses a Trojan Horse malware to get a backdoor access to one of the RAS controllers. Once malware is installed, the attacker gets control of the RAS controller whenever he desires. This includes outside the LAN of the RAS controller as well. Specifically, the malware provides undetectable communication between the attacker and the device, and provides attacker the ability to execute commands in the affected device. Once the malware installation is successful, we perform the coordinate cyber-attacks by replacing the existing RAS controller script with a malicious one which plays with a generator to damage the system. This part is intended to demonstrate the dangers of the malware in smart grids.

In the second part, the defense scheme against the malware attack is proposed. The main idea is to detect and disable the device operating for RAS controller that is affected by some type of malware. This is done by introducing the one other device called Overseer. The Overseer should not have any access or control over any part of the actual grid (relays, generators, etc.). However, it should be able to communicate with all RAS controllers. RAS controllers are also upgraded so that they will take an extra measurement from a randomly selected generator which is reported to the Overseer with all the other measurements they normally take periodically. The main task of the overseer is to oversee the RAS controllers by taking updates from them. Through the usage of the proposed architecture, the overseer can detect a RAS controller which is acting maliciously. Once the malicious controller is detected, it can disable it using denial of service (DOS) attack on it until the situation is fixed. It is to be noted that the smart grid requires RAS controllers to perform corrective action during disturbances in the grid, they are just there to keep track of the grid during normal functioning of the power system. This means that grid does not need RAS controllers to function normally. Another possibility is when the Overseer is infected. Since Overseer has no access/control over the grid, the worst thing an attacker can do is to DOS a RAS controller which, again, will not affect the grid.