

Modeling Security Policies for Mitigating the Risk of Load Altering Attacks on Smart Grid Systems

Abstract

While demand response programs achieve energy efficiency and quality objectives, they bring potential security threats into the Smart Grid. An ability to influence load in the system provides the capability for an attacker to cause system failures and impacts the quality and integrity of the power delivered to customers. This paper presents a security mechanism that monitors and controls load according to security policies during normal system operation. The mechanism monitors, detects, and responds to load altering attacks. The authors examined security requirements of Smart Grid stakeholders and constructed a set of load control policies enforced by the mechanism. A proof of concept prototype was implemented and tested using the simulation environment. By enforcing the proposed policies in this prototype, the system is maintained in a safe state in the presence of load drop attacks.