Abstract

As optimization, user capabilities, and data-taking abilities are incorporated into next-generation power grids, or smart grids, they face cyber threats. The traditional electrical grid could only be damaged by physical attacks; however, the smart grid can suffer remote/cyber attacks, which have not been studied extensively in the literature. The electrical grid forms the backbone of the modern society and its security has significant implications in military settings. This paper applies game theory to model three-levels (power plants, transmission, and distribution networks) of defenses and attacks in smart grid network security. We characterize both the attacker and the defender (who interact at three network levels: distribution, transmission, and power plants) best responses and equilibrium strategies. We find that the defender's best response is not only a function of direct attacks but also of the spread from connected networks. Sensitivity analyses of the equilibrium strategies show that when success probability of an attack against power plants reaches a threshold, the defender increases defending efforts for power plants. In contrast, the attack effort at all levels is not affected by this probability. This paper provides some novel insights to modeling and analyzing the emerging threats to the growing smart grid networks.

Citation

Shan, X. and J. Zhuang. "A Game-Theoretic Approach to Modeling Attacks and Defenses of Smart Grids", Reliability Engineering & System Safety, available online, 2019.