A Game-Theoretic Approach to Modeling Attacks and Defenses of Smart Grids

Giovanni Madejski\textsuperscript{a}, Xiaojun Shan\textsuperscript{a}, Jun Zhuang\textsuperscript{a}, Nageswara S. V. Rao\textsuperscript{b}

\textsuperscript{a} Department of Industrial and Systems Engineering \textsuperscript{b} Oak Ridge National Laboratory

Abstract

As optimization, user capabilities, and data-taking abilities are incorporated into the power grid, the next generation power grid, or smart grid faces the new risk of cyber threats. With the current electrical grid, physical access is required to cause damage, while with the smart grid it will be possible for users to remotely attack and severely damage the grid. We propose the use of a game-theoretic model to model three-levels of defenses and attacks (Power Plants, Utility Companies, and Home Networks) in smart grid network security. To our knowledge, such an approach to smart grid network security has never been taken, our paper fills this gap by characterizing both the defender’s and attacker’s best response functions and the corresponding Nash equilibrium. We find that the defender’s best response is not only a function of direct attacks but of the spread from connected networks. Sensitivity analysis of the equilibrium shows that when success probability of an attack against power plants reaches a certain threshold the defender increases defending efforts for power plants. In contrast, the attack effort at all network levels is not a function of this probability.

Notation

\( a_k \in \{0, 1, \ldots, n_k \} \) - Number of nodes in network of type \( k \) attacked
\( d_k \in \{0, 1, \ldots, n_k \} \) - Number of nodes in network of type \( k \) defended
\( P_k (a_k, d_k) \) - Probability of Network of type \( k \) operating
\( I_k \) - Indicator function that attacks outweigh defenses at network of type \( k \)
\( u_k \) - Defender’s Utility function
\( h_k \) - Attacker’s Utility function

Illustrations

- Smart Grid is large complex network, Figure 1 shows a network schematic highlighting essential components [1]
- Power is generated at power plants (Grandfather network) then transmitted to Utility companies (Father Network) and then finally arrives at the Home network (Child Network).
- Advanced Metering Infrastructure (AMI) is the underlying structure of the smart grid, the function of which is to monitor real-time power usage. This allows power generation and transmission to be controlled based on real-time demand.
- Alternative energy sources such as solar panels, personal generators, and plug-in electric cars help curb peak-time demand.

References