Alloy-based Game-theoretic Framework for Analyzing Security Issues in Small-scale Smart Grid Systems

Jianye Hao
Massachusetts Institute of Technology

Background and Motivation

Small-scale smart grid systems usually consist of a networked group of distributed energy resources including solar panels and wind turbines, which provide electric energy to small geographical areas. The system is highly dynamic and complex due to the complex interactions between different components, and thus highly vulnerable to malicious attacks. Efficient modeling and analysis approaches are needed to facilitate the system designers to design effective defending strategies to protect the system from being attacked by malicious attackers.

Game theory and formal verification are two promising techniques which can be applied to enhance the security of smart grid systems due to the following reasons. First, in small-scale smart-grid systems, due to the heterogeneous and distributed features, it is natural to apply game-theoretic approach to model the strategic interactions among different components, where each actor (e.g., energy provider, energy consumer, and malicious attacker) can be modeled as a self-interested player to maximize its individual utility. Second, given the system model and the strategies of the players, we would like to analyze the utilities of the players and whether certain desirable (safety/security) property of the system can be guaranteed. Given the highly dynamic and complex nature of the system, the formal verification tools (e.g., Alloy analyzer) usually provide expressive logical languages to describe various properties and support the automatic verification of those properties by taking into consideration all the possible states of the system.

Proposed Framework

We propose the following game-theoretic learning framework based on Alloy analyzer to investigate the security issue in small-scale smart grid systems, as shown in Figure 1. We model the security problem as an N+1 player *repeated Stackelberg game* where there exist N defenders (e.g., the energy providers) and one malicious attacker. At each round, the defenders first determine their defend strategies simultaneously and then the attacker will make its choice given the defending strategy profile of the defenders. Given the strategies of all players, the Alloy analyzer serves as the automatic computational tool to determine the utilities or check the satisfiability of certain property for the players.

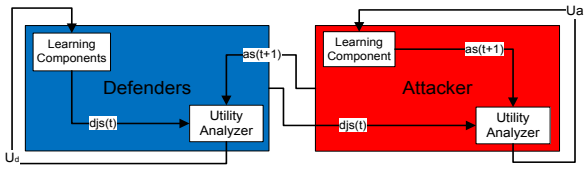

Figure 1 The overall game-theoretic learning framework

The possible inputs of the learning component are the strategy of the rest of players at the previous time step and the analyzing results from the Alloy analyzer. We would like to investigate the learning dynamics of the players within this learning framework. *One important question is to investigate whether and how the players are able to finally converge to certain stable strategy profile (e.g., Stackelberg equilibrium) such that certain desirable security state (or security property) of the system can be guaranteed.*

We will apply the previous framework to the practical small-scale power distribution network, and one particular example is shown in Figure 2. From the defender's perspective, each defender should determine whether it should invest resources to protect its corresponding facilities. From the attacker's perspective, it can launch either physical attack (e.g., attack transmission line) or cyber-attack (e.g., manipulate the data sent from the sensors) to compromise the function of the power distribution system. When some fault happens after the attack, the network operator will make the reconfiguration plan based on the feedback collected from the local fault detection sensors. The reconfiguration plan would directly affect the individual utility of each defender (energy supplier).

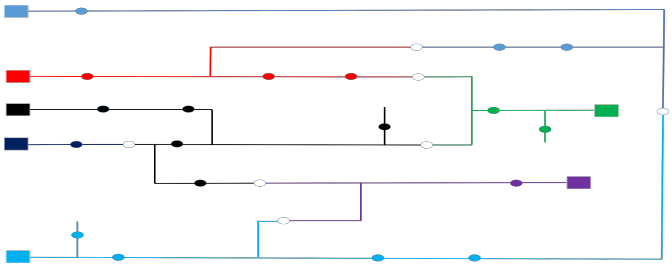

Figure 2 An example of power distribution system

One goal is to investigate how the defenders can learn to converge to a desirable defending strategy profile such that the overall system can reach a desirable security state (or certain security property can be guaranteed). We are also going to investigate possible incentive mechanism to incentivize the selfish defenders to invest more in protecting the network to increase the security of the overall grid system. We believe that our framework can provide valuable insights and guidance for implementing secure and reliable smart-grid systems.