Speaker: Saurabh Amin, MIT

Title: Some Structural Results on Network Security Games

Abstract:
This work focuses on the analysis of attacker-defender interactions on distribution networks (DNs) using game-theoretic tools. Two attack models are considered: (i) strategic disruption of network links; (ii) manipulation of distributed generation (DG) nodes.

In the first model, the defender chooses flow routing strategies to maximize the expected effective flow between source-destination pairs while facing strategic link disruptions and faces transportation costs. The attacker simultaneously disrupts one or more links to maximize her value of lost flow and faces cost of disrupting links. This game is strategically equivalent to a zero-sum game. Linear programming duality and the max-flow min-cut theorem are applied to obtain properties that are satisfied in any mixed Nash equilibrium. In any equilibrium, both players achieve identical payoffs. While the defender's expected transportation cost decreases in attacker's marginal value of lost flow, the attacker's expected cost of attack increases in defender's marginal value of effective flow. Interestingly, the expected amount of effective flow decreases in both these parameters.

In the second model, the defender observes and responds to the adversary induced DG node disruptions by imposing partial load shedding and controlling supply. The loss to the defender includes loss of voltage regulation and cost of induced load control under supply-demand mismatch caused by the attack. Solving this sequential game is hard due to nonlinear power flows and mixed-integer decision variables. To address this challenge, the problem is approximated by tractable formulations based on linear power flows.

The set of critical DG nodes and the set-point manipulations characterizing the optimal attack strategy are characterized. An iterative greedy approach to compute attacker-defender strategies for the original nonlinear problem is proposed. These results also provide guidelines for optimal security investment and defender response in pre- and post-attack conditions, respectively.
