CAREER: Resilient Design of Networked Infrastructure Systems: Models, Validation, and Synthesis

PI: Saurabh Amin (Massachusetts Institute of Technology), email: amins@mit.edu

Objectives

To develop a design framework that integrates resiliency improving tools (detection and control) and incentives schemes for CPS deployed in civil infrastructure networks.

Focus:

- Vulnerability assessment to cyber-physical failures (faults/attacks)
- Tools to detect and respond to both local and network-level failures
- Information systems and incentive schemes to improve network performance under failures, while accounting for interaction between strategic entities.

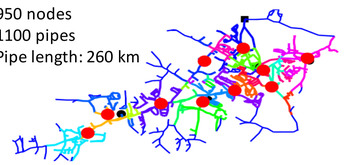
Relevant papers:

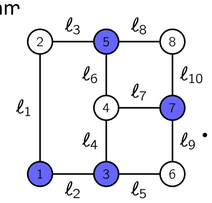
- "Network sensing for security against link disruption attacks" (with M. Dahan & L. Sela), Allerton 2016
- "Effects of information heterogeneity in bayesian routing games" (with J. Liu & G. Schwartz), *submitted*
- *"Sensor placement for fault location identification in water networks: A minimum test cover approach" (with L. Sela, W. Abbas & X. Koutsoukos), Automatica 2016*
- *"Security assessment of electricity DNs under DER node compromises" (with D. Shelar), IEEE TCNS 2016*

Network Sensing for Fault Diagnostics

- **Objective:** For a given network, find minimum number of sensors and their placement, so that each link is monitored by at least one sensor: **Minimum Set Cover (MSC).**
- **Approach:** Augmented Greedy Algorithm

- 950 nodes
- 1100 pipes
- Pipe length: 260 km

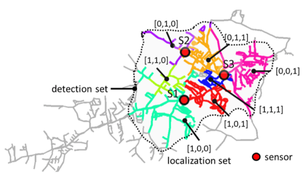




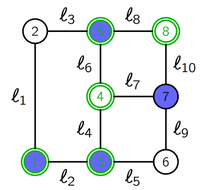
- MSC for one-hop sensing.

Fault Detection versus Localization

- **Objective:** For a given network, find minimum number of sensors and their placement, so that each link failure is isolated (identified): **Minimum Test Cover (MTC).**
- **Approach:** Greedy algorithm extended to approximate the MTC.



Adopted from Jolly et al 2014



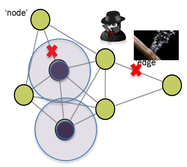
- MSC and MTC for one-hop sensing.

Joint work with L. Sela, W. Abbas, X. Koutsoukos

Network Sensing for Attack Detection

Strategic game on a flow network:

- **Network operator** (defender): chooses a sensor placement to maximize the number of failures that are detected.
- **Attacker:** disrupts one or more links simultaneously to maximize the number of failures that remain undetected.



Features of the model:

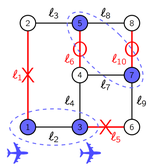
- General sensing model that allows heterogeneous range.
- Focus on randomized strategies based on mixed Nash equilibria.
- Characterization of the support of equilibrium strategies in terms of minimum set cover and maximum set packing.

Duality of Attacker and Defender Problems

In equilibrium:

- The defender randomizes over a **minimum set cover.**
- The attacker randomizes over a **maximum set packing** (set of "sensing independent" links of maximum size).

The LP relaxations of the minimum set cover and the maximum set packing problems a re dual from each other.

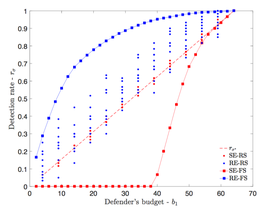


- Nash equilibrium for one-hop sensing

Optimal Sensing Strategies

Theorem:

- In equilibrium, both players' payoffs can be bounded using both players' amount of resources and the size of the minimum set cover and maximum set packing.
- The defender's strategy guarantees a tight lower bound on the fraction of failures that are detected.

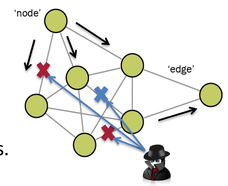


Joint work with M. Dahan and L. Sela

Network Flow Routing under Link Disruptions

Strategic game on a flow network:

- **Network operator** (defender): routes feasible flow through the network to maximize her value of effective flow but faces transportation costs.
- **Attacker:** disrupts one or more links to maximize her value of lost flow but also faces cost of disrupting edges.



Features of the model:

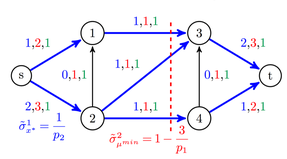
- Strategic routing to maximize effective flow net transportation cost.
- No rerouting of flow after attack.
- The model enables identification of vulnerable links.

Duality of Attacker and Defender Problems (revisited)

In equilibrium:

- The defender randomizes over a **min-cost max-flow** of the network.
- The attacker randomizes over a **min-cut set** of the network.
- Both players' payoffs and the amount of effective flow can be computed in closed form using complementary slackness.

The maximum flow and the minimum cut set problems are dual from each other.

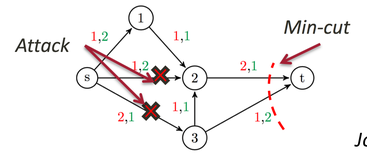


- Nash equilibrium.

Vulnerability to Strategic Disruptions

Theorem:

- In equilibrium, any link that is attacked with a positive probability must be saturated by every min-cost max-flow. Such a link is called **vulnerable**.
- The fraction of such links defines a vulnerability metric.
- The set of vulnerable links includes all the links that are part of a **min-cut set**.



Joint work with M. Dahan

Vulnerability to Strategic Disruptions

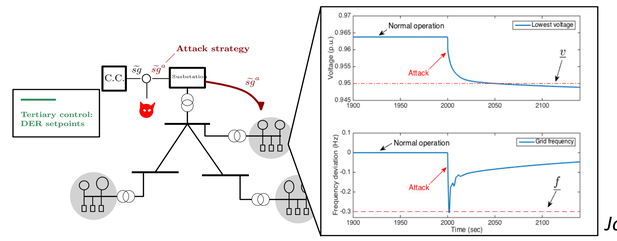
Theorem:

- In equilibrium, any link that is attacked with a positive probability must be saturated by every min-cost max-flow. Such a link is called **vulnerable**.
- The fraction of such links defines a vulnerability metric.
- The set of vulnerable links includes all the links that are part of a **min-cut set**.

Vulnerability of Distribution Nets to DER Disruptions

Distribution networks with vulnerable Distributed Energy Resources (DERs):

- Attacker introduces incorrect DER set-points by manipulating CC communications to introduce loss of voltage regulation, load shedding, and power quality
- Defender responds by performing centralized (or distributed) network control

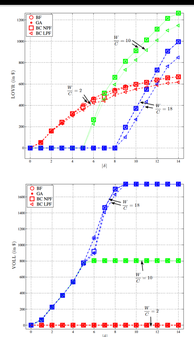


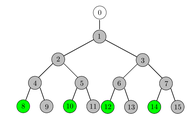
Joint work with D. Shelar

Attacker-Defender Interaction as Sequential Game

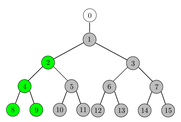
Theorem:

- Optimal attack plans show downstream preference
- When cost of load control is high, defender permits loss of voltage regulation
- For low intensity attacks, load control is preferred
- For high intensity attacks, load control may not not effective
- Design 1 is more secure than Design 2





Design 1



Design 2

This work is supported by the NSF sponsored projects CNS 1453126 and CNS-1239054.