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 of 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

Solution approach

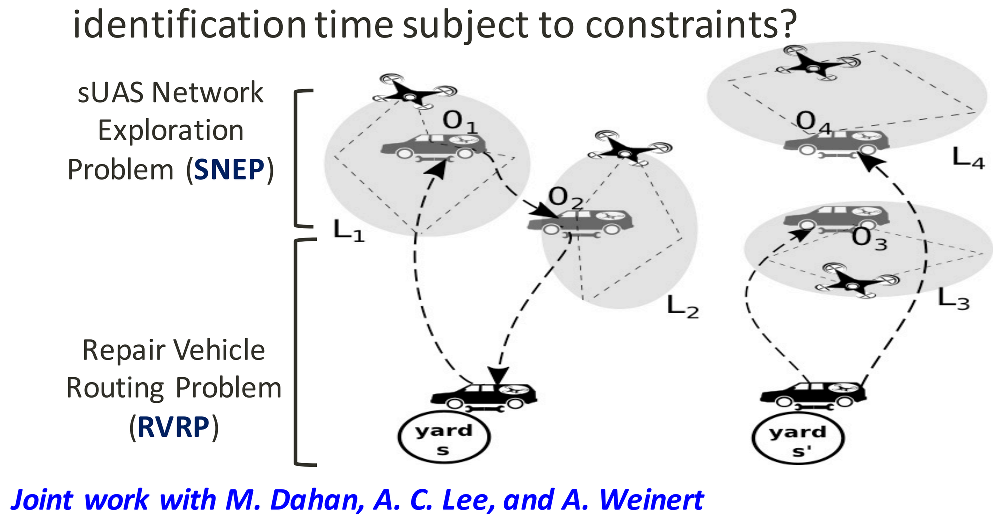
- Study equilibrium properties of operator-attacker game
- Construct an ε-Nash equilibrium based on solutions of:
  - Minimum Set Cover [MSC]: Operator strategy is to randomize over MSC
  - Maximum Set Packing [MSP]: Attacker strategy is to randomize over MSP
- Compute an approximate solution of the MPEC:
  - # of sensors with optimality gap
  - Guarantee(s) on detection performance

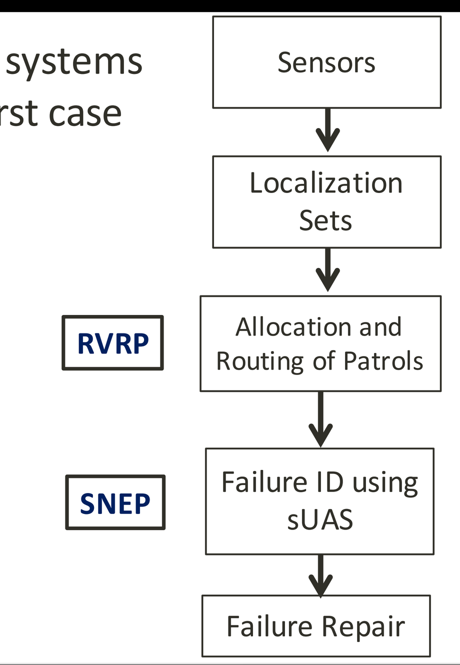
Main advantages:

- Scalable to very large networks
- Small optimality gap in most practical cases
- When |MSC|=|MSP|: We obtain an exact solution, and generalize some classical results on hide-and-seek and network security games
- Does not require an exact knowledge of the attacker's resources

Tasking mobile sensors for network monitoring

Question: How to optimally allocate and route mobile sensing systems to identify failures within localization sets, to minimize the worst case identification time subject to constraints?





Joint work with M. Dahan, A. C. Lee, and A. Weinert

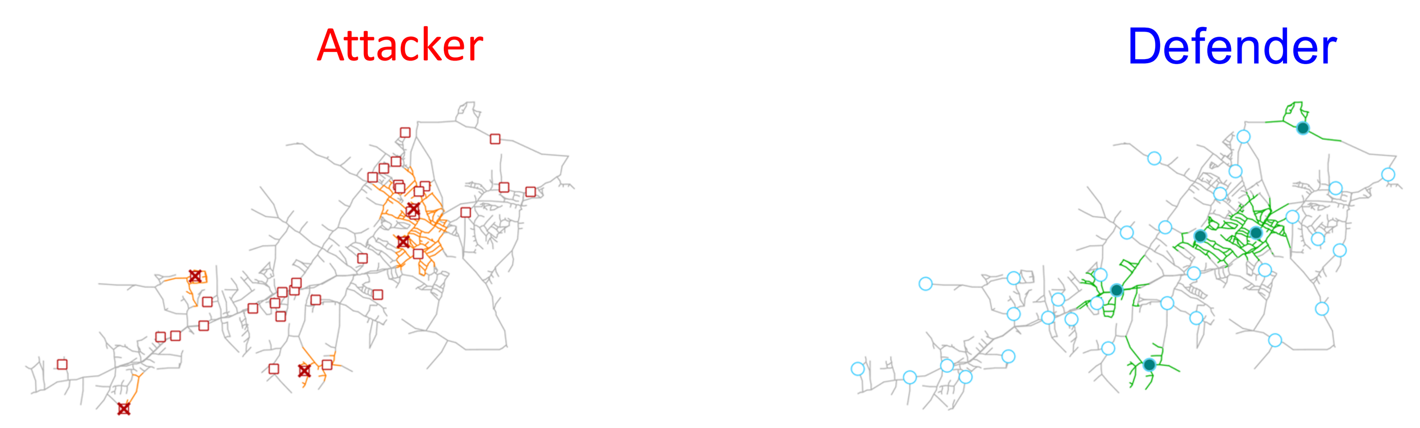
Major topics

I. Value of information systems in strategic environments
(a) Effects of information heterogeneity in traffic congestion games
(b) Value of intrusion detection systems in limiting non-technical losses in electricity networks (e.g., energy fraud)

II. Optimal resource allocation in large-scale networks
(a) Monitoring random and strategic disruptions (water & gas)
(b) Deployment of distributed energy resources (DERs) to improve resilience of electricity networks

III. Control/routing with unreliable or insecure components
(a) Freeway traffic control under stochastic capacity, or incidents
(b) Network routing under disruptions induced by adversarial manipulations to sensor-control data

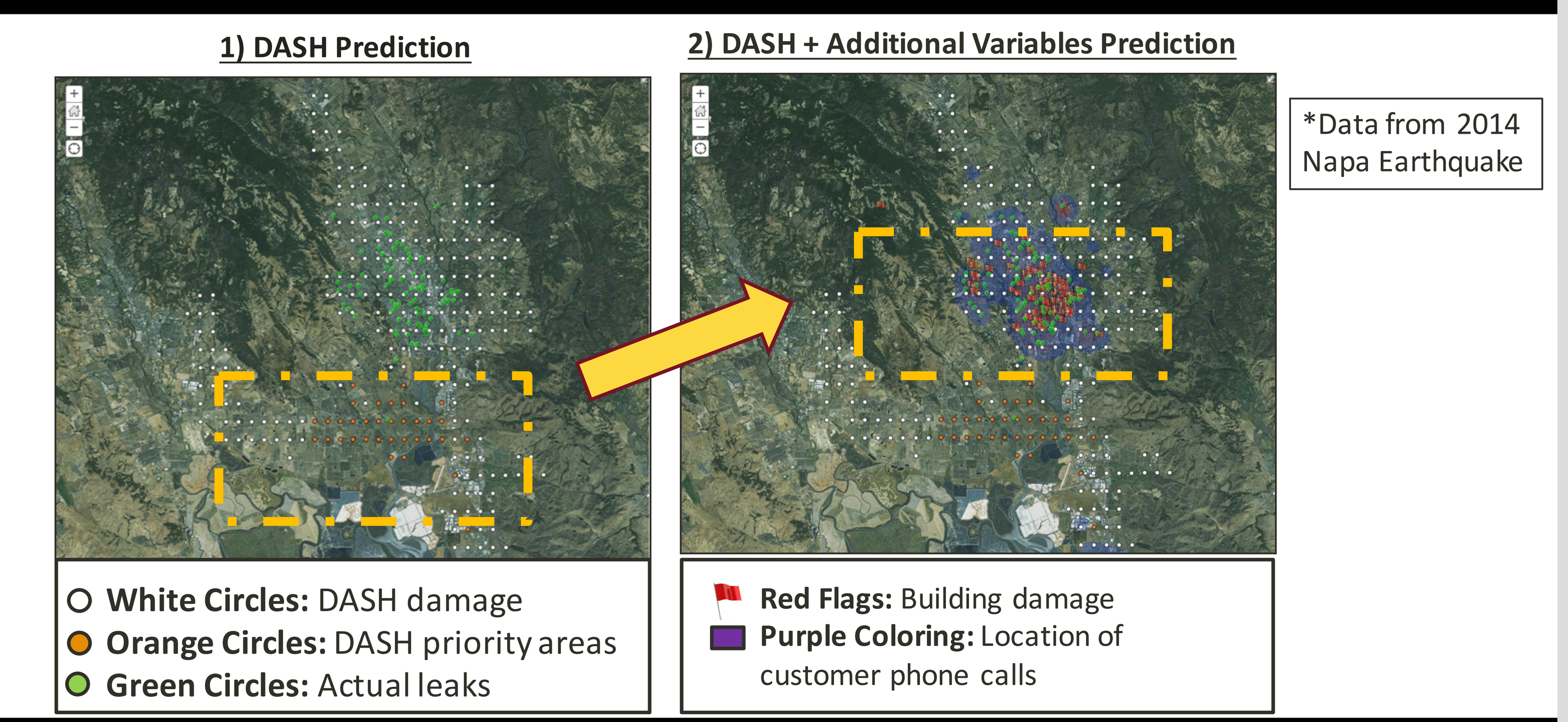
MSC-MSP based strategy profile



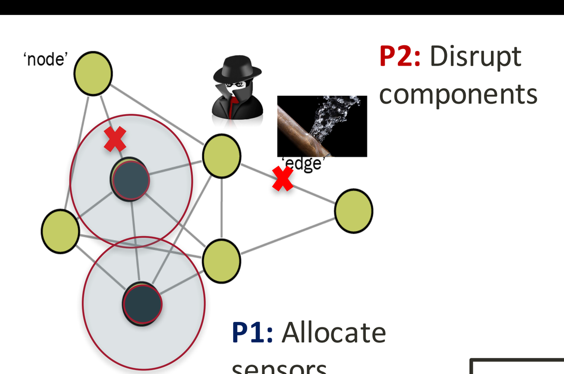
MSP: Maximum set of edges that are covered by any node at most once

MSC: Minimum set of nodes that cover all edges

Extension 2: Damage localization after earthquake



II.(a) Monitoring under strategic disruptions



- Strategic interaction
- Resource limitations
- Very large (combinatorial) action sets
- Dynamic and asymmetric information

Applications:

- Hide-and-seek games
- Network security
- Search and surveillance
- **Infrastructure defense**

Our focus: Allocation of sensing resources in adversarial environments

- Incorporate a generic sensing model
- Ensure desirable performance (detection rate)
- Compute optimal (equilibrium) allocation

Main ideas

Main case of interest: large network and limited resources

- (# of sensing resources) < |MSC| *and* (# of attack resources) < |MSP|

Two tools:

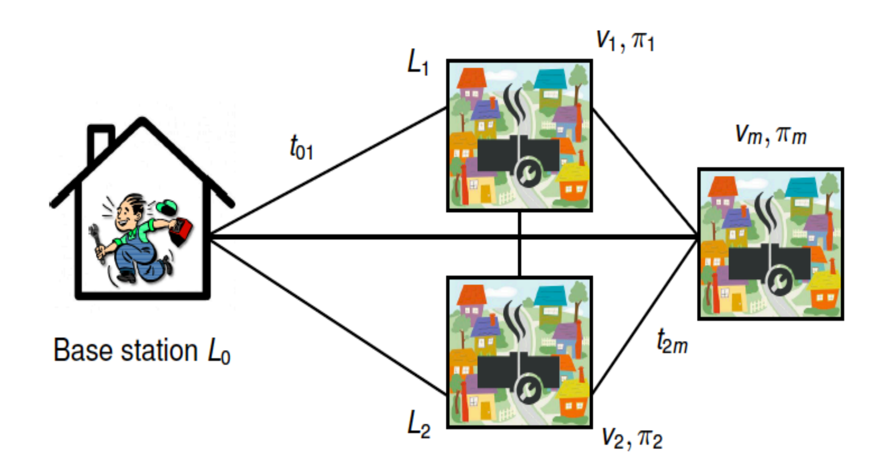
- Strategic equivalence of zero-sum games:
  - Linear programming (LP) duality, but LPs are too large to compute NE
- MSC (coverage) and MSP (spread):
  - Weak duality; both problems can be solved using integer programs

Three techniques:

- Construct MSC-MSP based strategy profile
- Exploit properties of sensing model:
  - Monotone submodular (w.r.t. sensor placements) and additive (w.r.t. attacks)
- NE properties: Both players randomize and each player uses all available resources. Also, sensing strategies in equilibrium "cover" the entire network

Monitoring under uncertain diagnostic information

Question: How to optimize the scheduling of monitoring resources under limited diagnostic information?



Our focus:

- New formulation involving stochastic orienteering and probing
- Solving it using non-adaptive and greedy approaches

Joint work with M. Dahan, S. Link, and Prof. G. Perakis

Monitoring problem

- Sensing model: detect or not based on location of sensors and components
- Attacker: simultaneous edge disruptions
- Operator: (randomized) sensing over subset of nodes
- **Objective**: Maximize # of detections (operator)
  Maximize # of undetected events (attacker)

Question: How many sensors are required and how to strategically allocate them in the network to detect adversarial attacks?

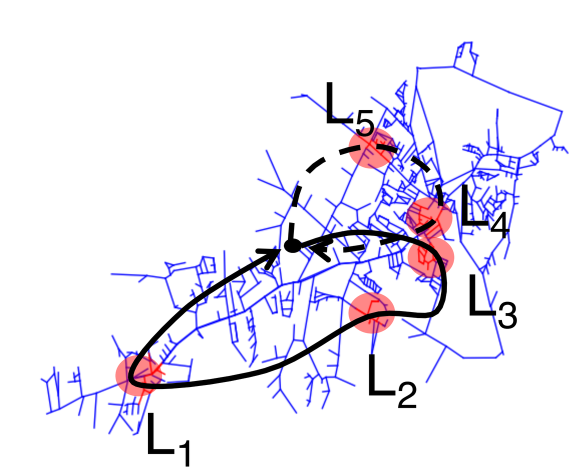
Formulation: Mathematical Program with Equilibrium Constraints (MPEC)
Minimize # of sensors to guarantee that:

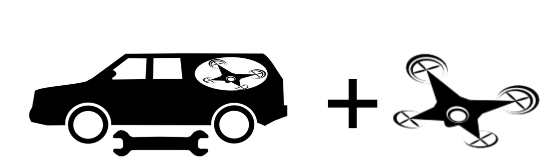
- Expected detection rate > threshold in *any* equilibrium of induced game

Joint work with M. Dahan, and Prof. Lina Sela (UT Austin)

Extension 1: sUAS-based network monitoring

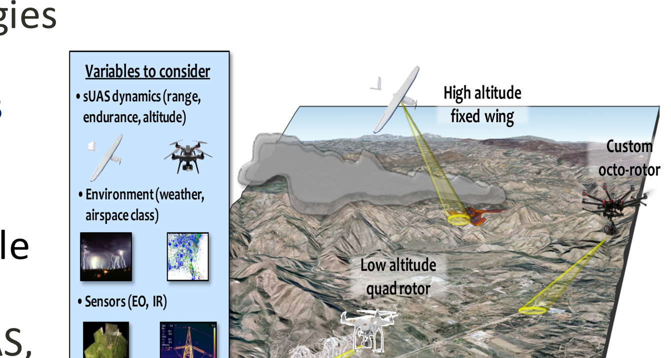
- Disparity exists between ideal monitoring and inspection, and current practices for utility networks (e.g., oil and gas)
- Inefficiencies and suboptimal allocation of resources lead to increased cost from losses in the case of failure events
- Mobile Sensing Systems with small Unmanned Aerial Systems (sUASs) is an opportunity to bridge this gap





Teaching: Capstone Project

- Beaver Work capstone project with MIT CEE Department
  - Course 1.013 **CEE Capstone in 2017**
  - Support: Lincoln Laboratory and Modern Technologies Solutions, Inc.
  - **Spill over to Graduate research and UROP projects**
- "Unmanned Aerial System (UAS) Sensor On-Demand" capability
  - System operator: I need sensors here => UAS enable data collection
- Prototype strategic tasker given the environment, sUAS, users, & sensors
  - Integrate sUAS system with mission specific algorithms & systems
  - Mission planning cognizant of sUAS constraints



This work is supported by the NSF projects CNS 1453126 and CNS-1239054. Results presented here are joint with M. Dahan, A. C. Lee, S. Link, A. Weinert (MIT LL), Prof. L. Sela (UT Austin), and Prof. G. Perakis (MIT)