Securing Mobile CPS against Stealthy Attacks

PI: Mina Guirguis – Texas State University

http://cs.txstate.edu/~mg65/mcps

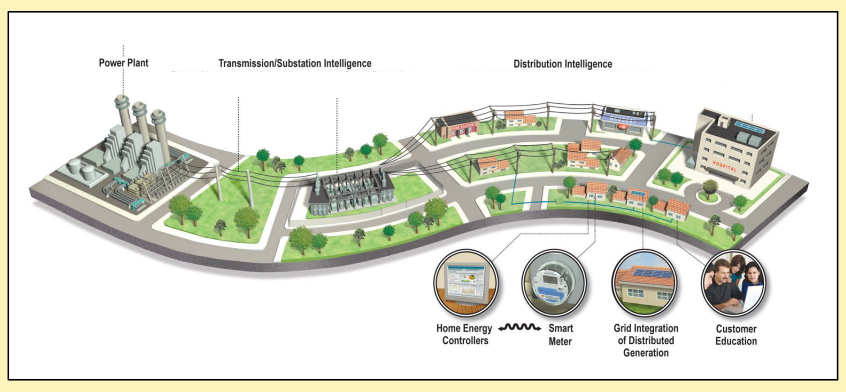
Motivation:

- Cyber-Physical Systems (CPS) will be pervasively integrated into our physical world
- How to ensure the security and safety of CPS?

Challenges:

- Reliance on wireless technology
  - Easy to jam and interfere with
- Complexity with real-time, energy and mobility constraints
  - Widens the malicious opportunities
- Attacks are not “random noise”, but are well orchestrated
  - Studies that focus on random noise and disturbance do not apply

Intelligent Transportation Systems – src: DoT

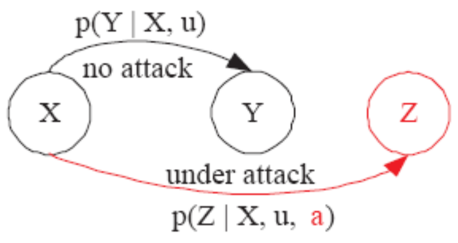


Smart power grid – src: DoE

Micro Aerial Vehicles – src: Air Force

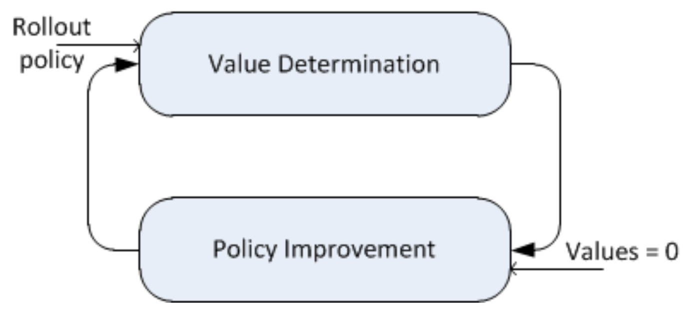
Methodology: Identifying Stealthy Attacks

- Attacker solves Markov Decision Problems
  - Aims to evolve the system into “bad” states (Z)
  - Pays a price when attacks
  - Gains a reward when inflicts damage
  - Identifies polices that maximize the cumulative rewards

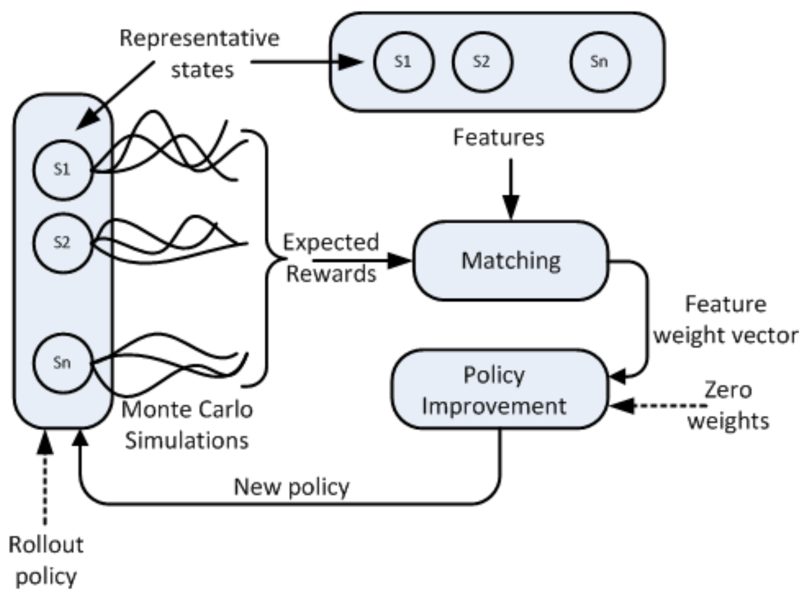


$$\max_{\mu_1,\mu_2,\ldots} E\left[\sum_{k=1}^{T} R(k)|I_k\right]$$

- The curse of dimensionality:
  - Large state space makes it computationally infeasible to obtain exact solutions [Bellman]

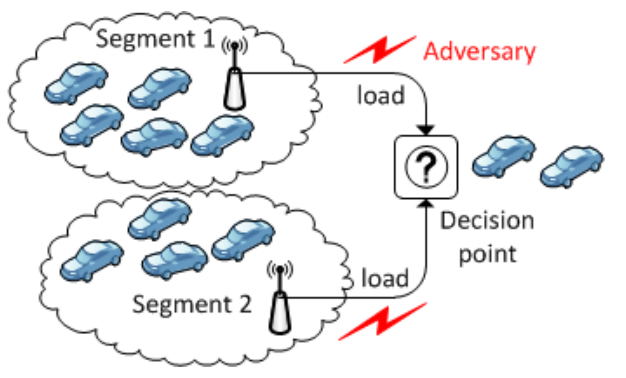


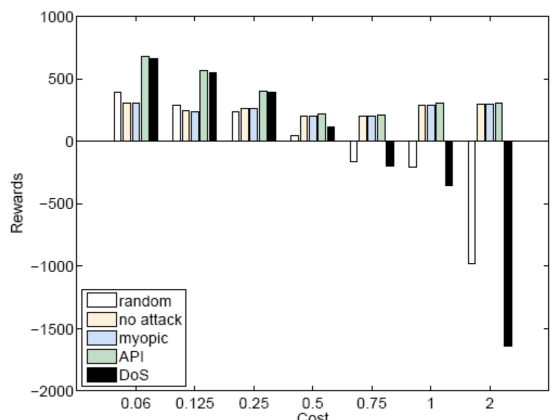
- Approximate Policy Iteration
  - Relies on Monte Carlo simulations
  - Characterizes states based on a set of feature
  - Uses a parametric cost-to-go approximation for the value function [Bertsekas]



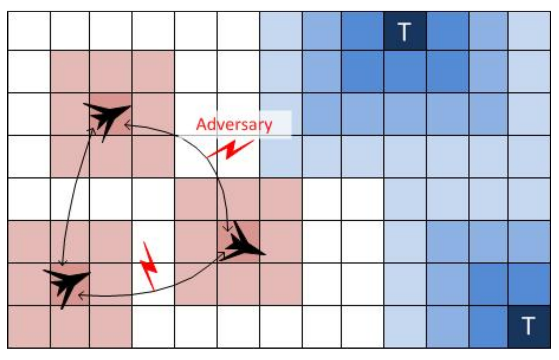
Instantiations of exploits:

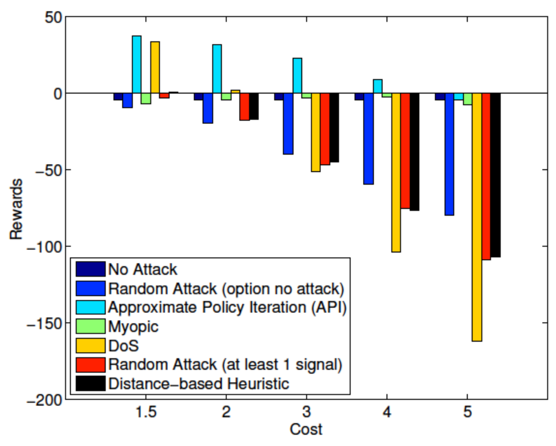
- Intelligent Transportation Systems



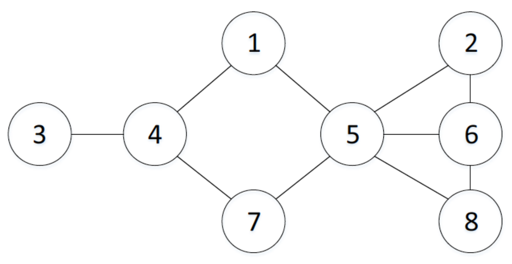


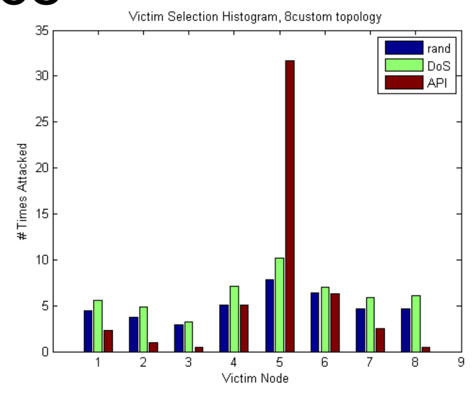
- Multi-agent Coordination Systems





- Wireless interference





Methodology: Developing Defense Strategies

- Game-theoretic approach
  - Zero-sum game between the defender (player 1) and the attacker (player 2)
  - Mixed strategies (X, Y) are obtained as solutions to various optimization problems

Attacker

Defender	Target 1	Target 2
Target 1	(4,-4)	(-1,1)
Target 2	(-5,5)	(2,-2)

$$\mathcal{A}_1 = \left\{a_1^1, a_1^2, \ldots, a_1^{2^N}\right\} \quad \mathcal{A}_2 = \{a_2^1, a_2^2, \ldots, a_2^{N+1}\}$$

- The curse of dimensionality:
  - Action spaces may be exponential in the number of the nodes

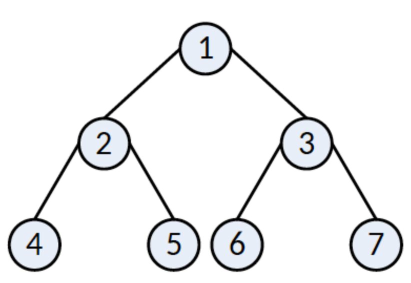
$$U_1 = \mathbf{X}^T\mathbf{R}_1\mathbf{Y} = \sum_{i=1}^{2^N}\sum_{j=1}^{N+1} x_i y_j R_1(a_1^i, a_2^j)$$

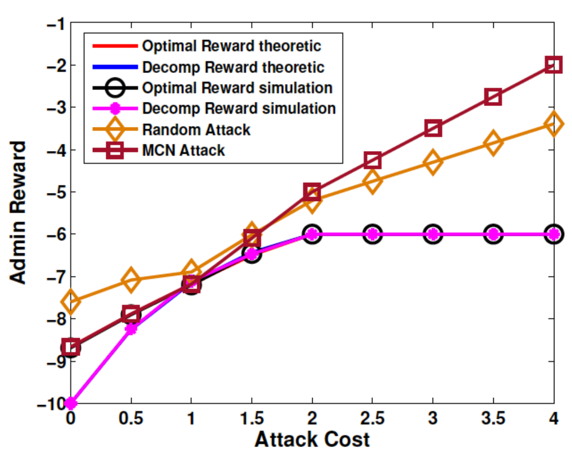
- Develop approximation methods:
  - Decomposition approach: solve a sub-game per node
  - Marginal approach: optimize over marginal variables bypassing the mixed strategy

$$\begin{aligned} &\underset{\mathbf{x}}{\text{maximize}} && U_1 \\ &\text{subject to} && \sum_{i=1}^{2^N} R_1(a_1^i, a_2^j)x_i \geq U_1, \quad \forall j = 1,\ldots,N+1. \\ &&& \sum_{i=1}^{2^N} x_i = 1, \\ &&& x_i \geq 0, \quad i = 1,\ldots,2^N. \end{aligned}$$

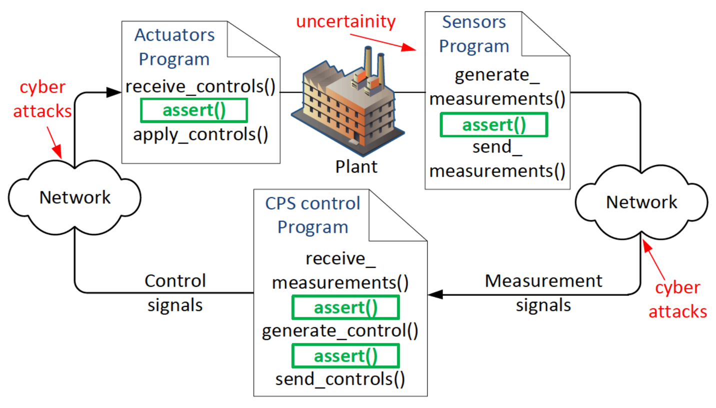
Instantiations:

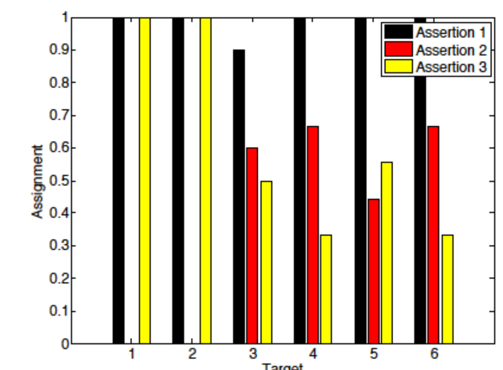
- Wireless Interference





- SCADA





Interested in meeting the PIs? Attach post-it note below!

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

National Science Foundation
WHERE DISCOVERIES BEGIN

TEXAS STATE UNIVERSITY SAN MARCOS
The rising STAR of Texas