Securing Mobile CPSs against Stealthy Attacks

PI: Mina Guirguis – Texas State University

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

Motivation:

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

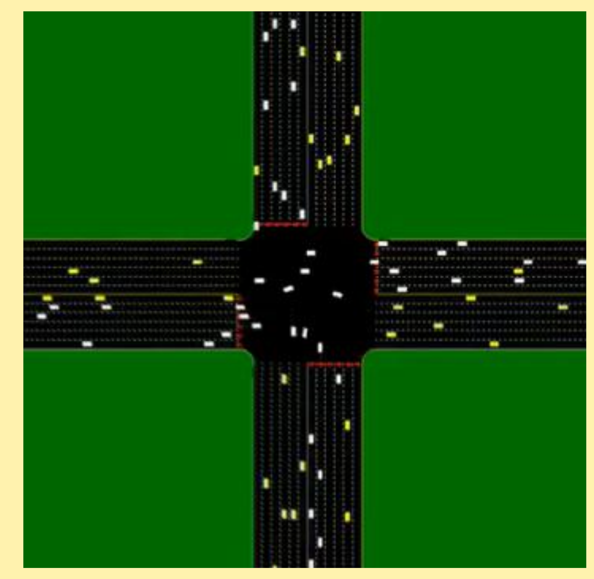
Challenges:

- 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

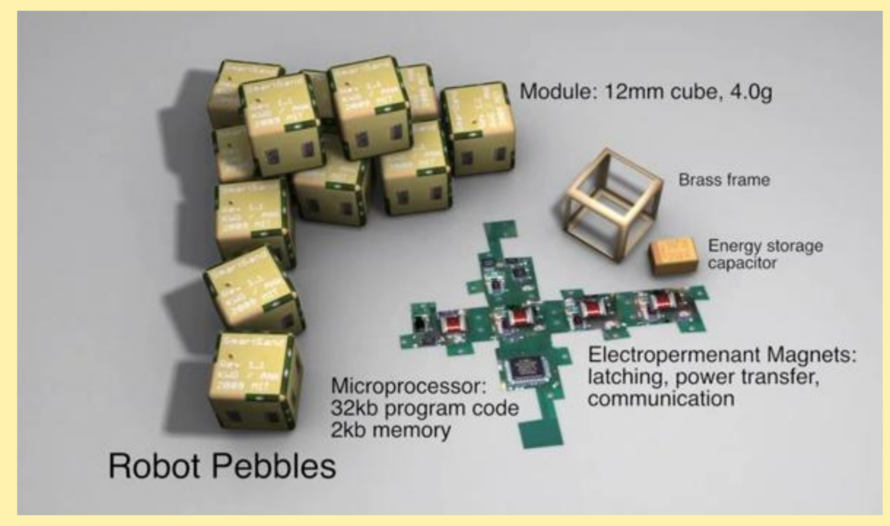
Scope of work:

- Identifying stealthy attacks
- Developing defense mechanisms

[European Commission- *swarmanoid*]



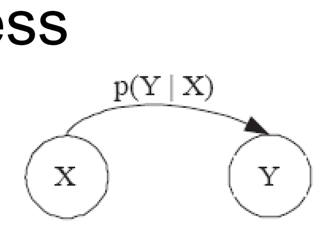
[UT- Multi-agent systems]



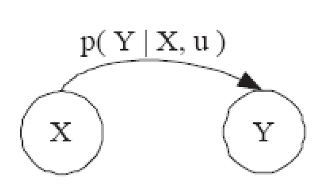
[MIT- Smart Sand]

Methodology: Identifying Stealthy Attacks

- Markov Decision Process
  - Sate of the system
  - Transitions

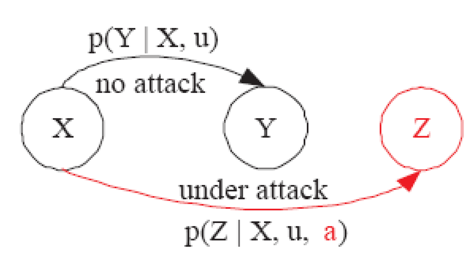


[independent]



[controlled]

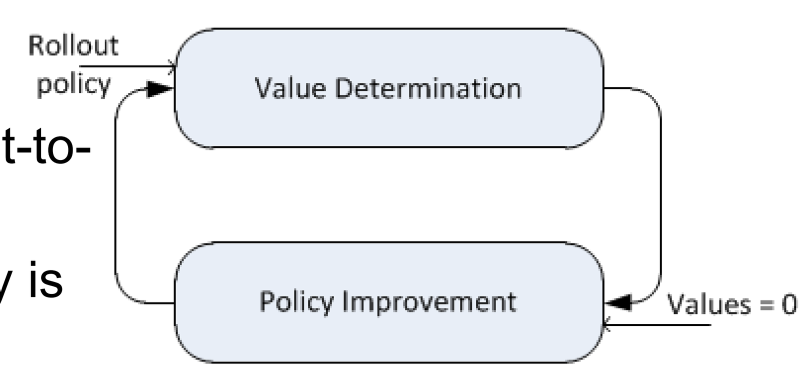
- Offense strategy
  - Aims to evolve the system into "bad" states (Z)
  - Pays a price when attacks
  - Gains a reward when inflicts damage
  - Identifies polices that maximize the cumulative rewards



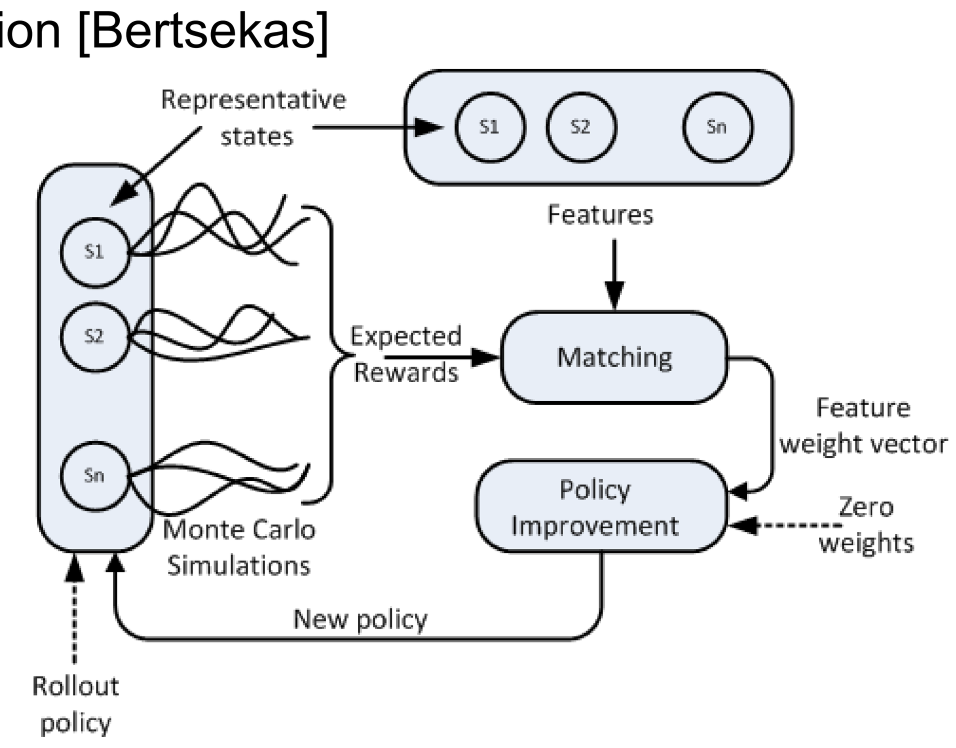
[under attack]

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

- Exact Policy Iteration
  - Optimal policies can be obtained
  - Value determination: expected cost-to-go values are computed
  - Policy improvement: a better policy is generated

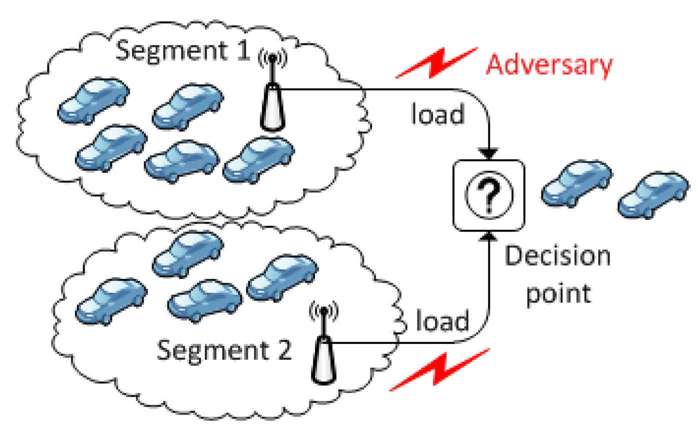


- The curse of dimensionality:
  - Large state space makes it computationally infeasible to obtain exact solutions [Bellman]
- Approximate Policy Iteration
  - Relies on Monte Carlo simulations
  - Characterizes states based on a set of feature
  - Uses a parametric cost-to-go approximation for the value function [Bertsekas]

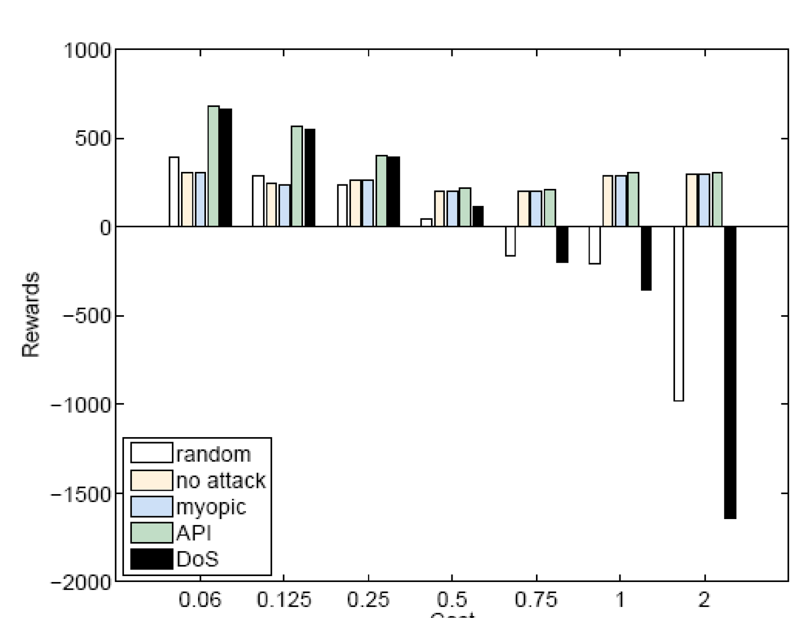


Stuck in Traffic (Sit) Attacks on Intelligent Transportation Systems

- The setup
  - Decision points reflect loads on segments
  - Drivers make informed decisions
  - Attackers aims to cause congestion



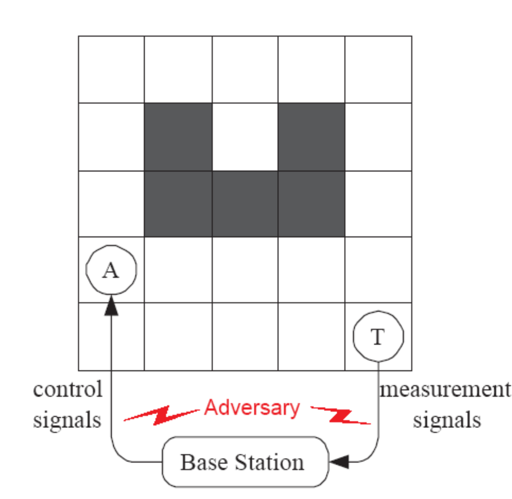
- Scenarios
  - Traffic optimization
- Damage
  - Degree of imbalance
- Cost
  - Number of vehicles affected



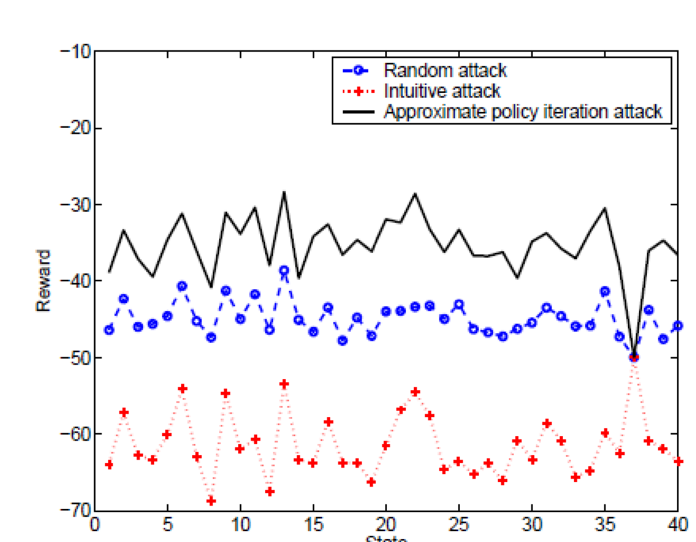
http://arxiv.org/abs/1210.5454

Stealthy Attacks on Target Tracking Applications

- The setup
  - Target moves randomly
  - Agent seeks to find the target
  - Attacker aims to hinder tracking



- Scenarios
  - Search and rescue
  - Border control
- Damage
  - Distance between the agent and the target
  - Negative if target is found
- Cost
  - Different values for control and measurement signals



Collaborators: George Atia (UCF), Vu Nguyen (Texas State), Janiece Kelly (Texas State) and Seth Richter (LeTourneau)

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

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD

TEXAS STATE UNIVERSITY SAN MARCOS
The rising STAR of Texas