Module on Network Security Games



Lina Sela, Mathieu Dahan, Jeff Liu, and Saurabh Amin

MIT Dept. of CEE & Center for Computational Engg.

Objectives

We developed a game theory module with focus on network security to teach UG/G students and professional engineers using interactive simulations of network games:

* Water network management
  * From single decision maker
  * To decentralized control
* Impacts of CPS failures
  * Disturbance propagation
  * Contaminant spread
* Strategic sensing & response
  * Game theory (network games)
  * Detection theory

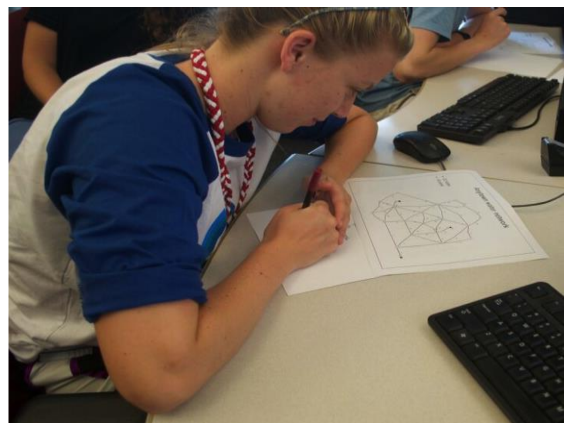
Network failures: bursts/leaks, contamination

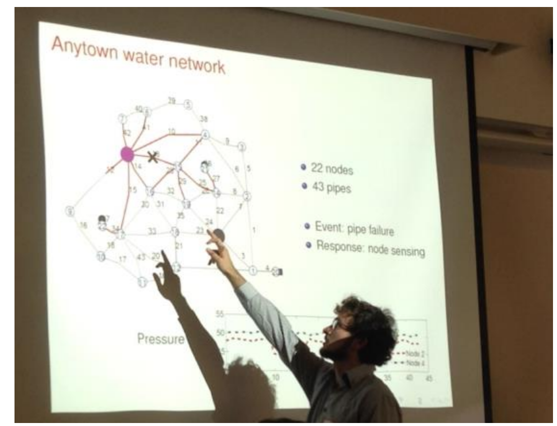
Water theft: California drought

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Offerings

- MIT Freshman Pre-orientation programs (Sept., 2015)
- Practitioners & professional engineers at Harvard Conf. (Oct., 2015)





- Upcoming:
  - "Game Theory for Infrastructure Security" to be offered during IAP 2016 to MIT Freshmen
  - Exercises will be included in UG Systems core subject: "Principles of Energy and Water Sustainability"

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Outline and Learning goals

1. Large-scale simulation of attack scenario on water networks
   * Real-world attack models
   * Effectiveness of defender (network operator) strategies
   * Simulations using EPANet
2. Decision theory
   * Game theory: Nash equilibrium, learning in games (fictitious play)
   * Computing equilibria: Prisoner's dilemma, matching pennies, …
   * Optimization: Set cover, facility location, network flow problems

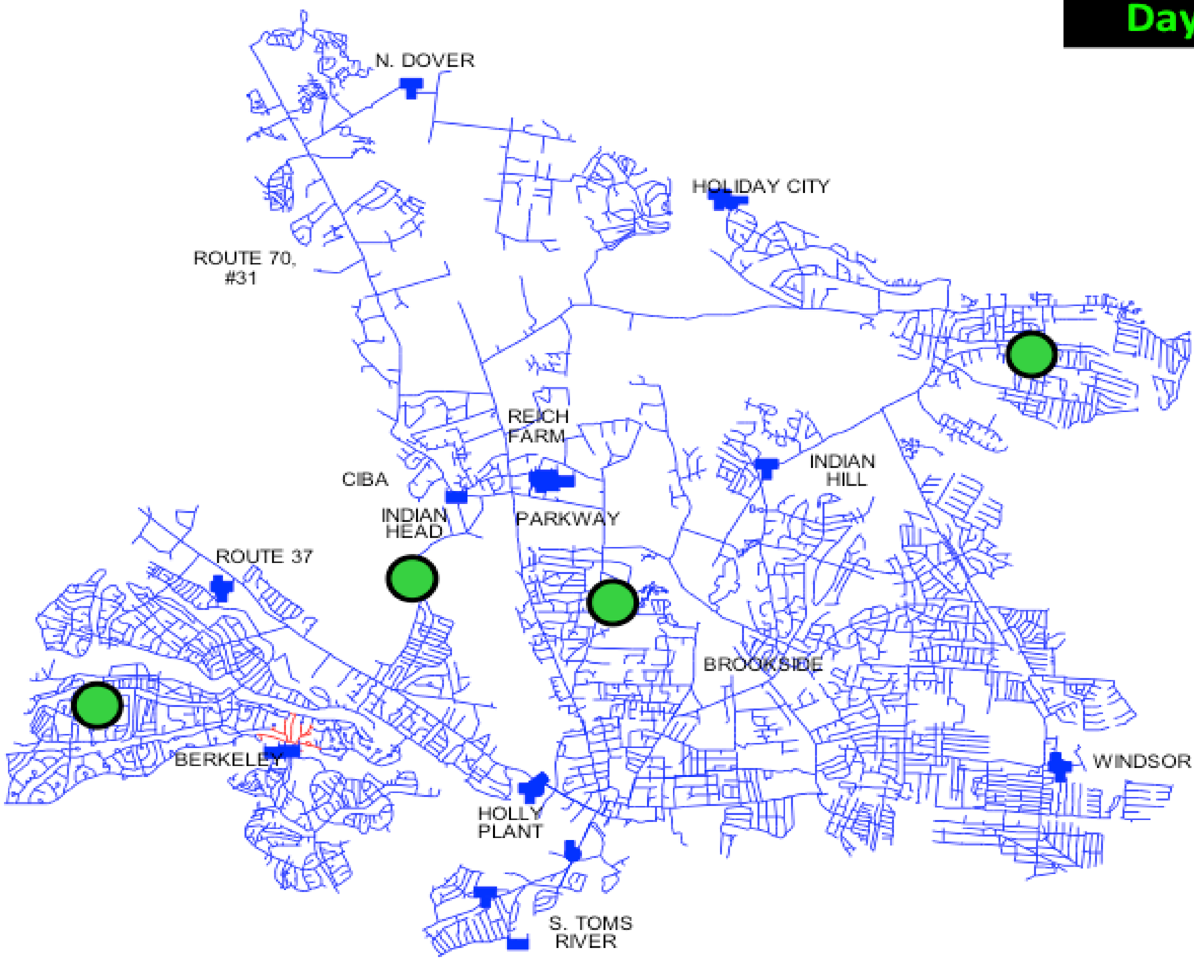
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Back-flow attack scenario on real-world networks

Dover, NJ

- Nodes: 14,945
- Pipes: 16,056
- Length: 484 [mi]

Day 1, 1:00am



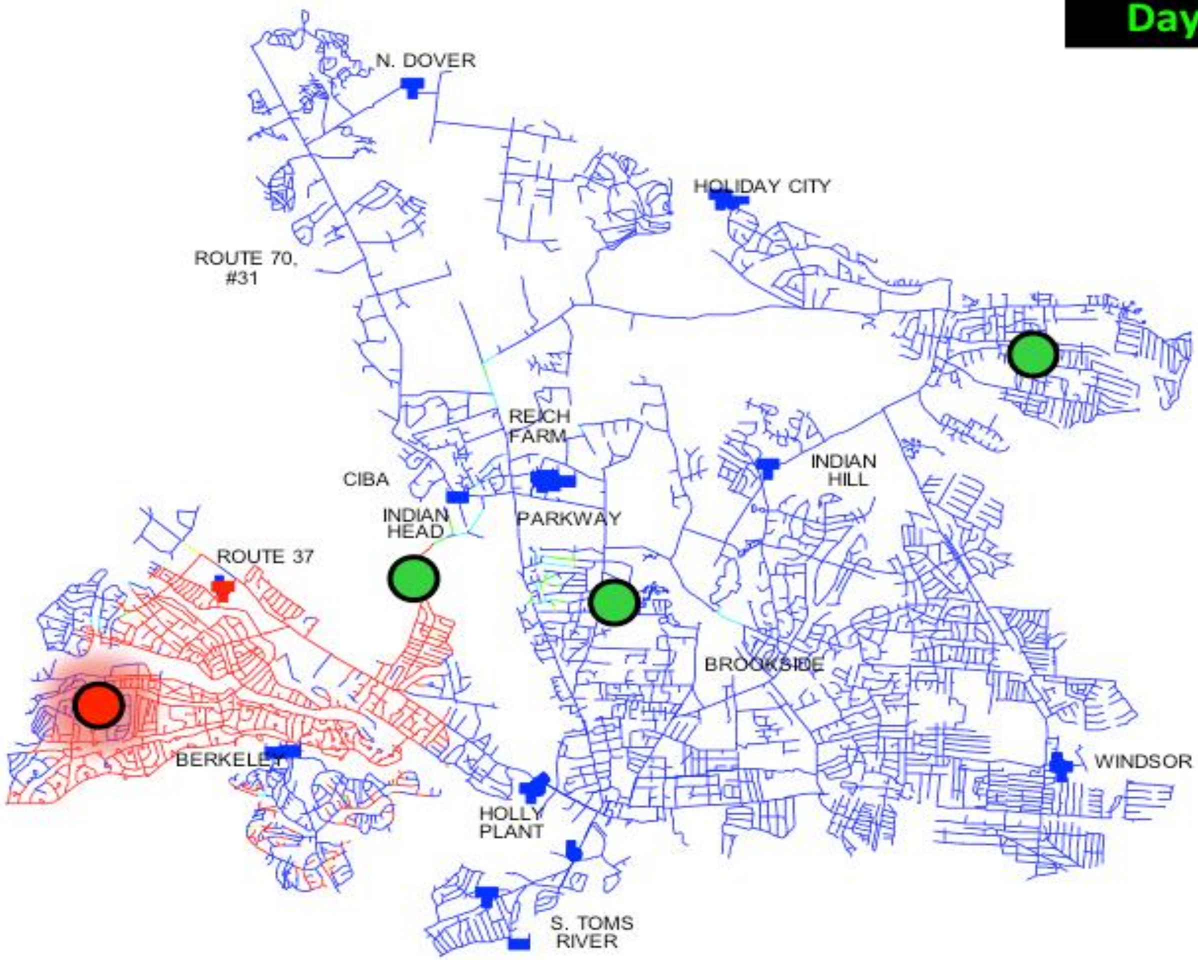
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Back-flow attack scenario: disturbance propagation

Dover, NJ

- Nodes: 14,945
- Pipes: 16,056
- Length: 484 [mi]

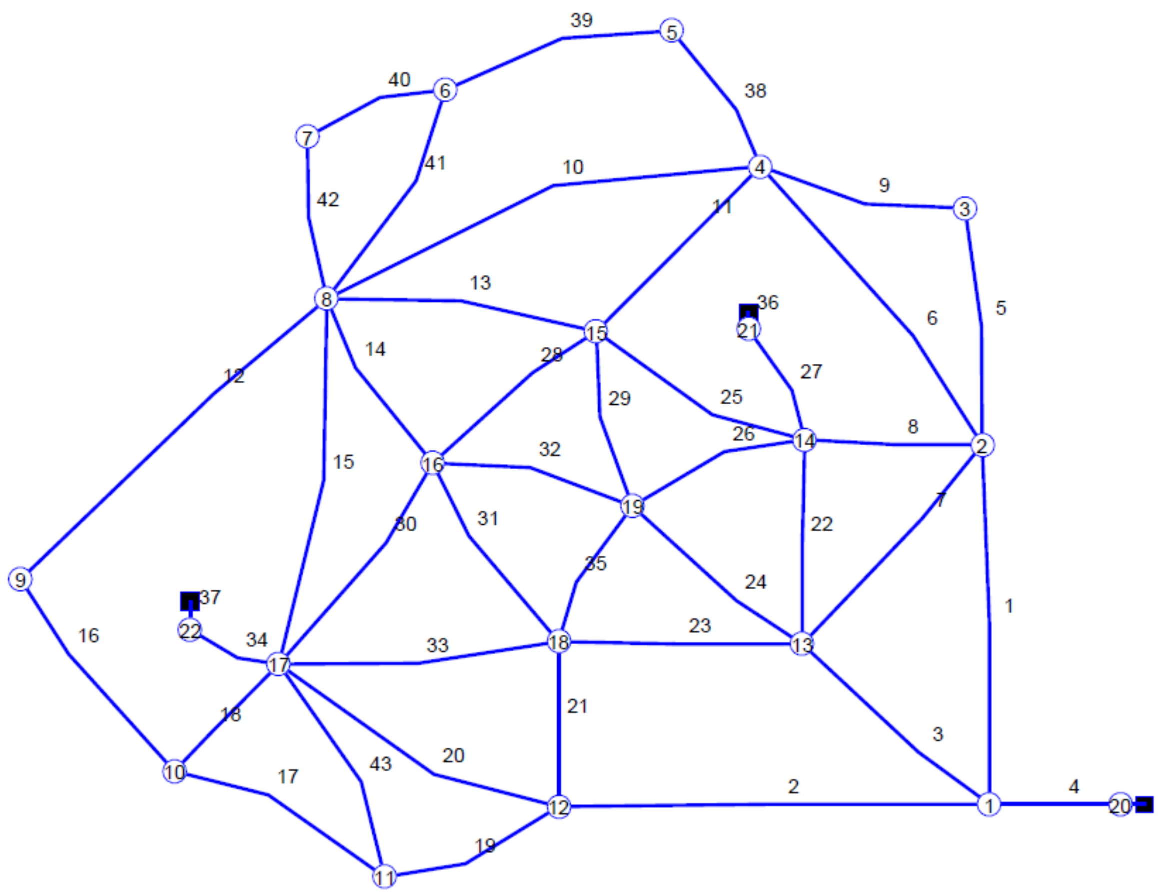
Day 1, 8:00pm



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Decision theoretic concepts using benchmarks: Anytown water network

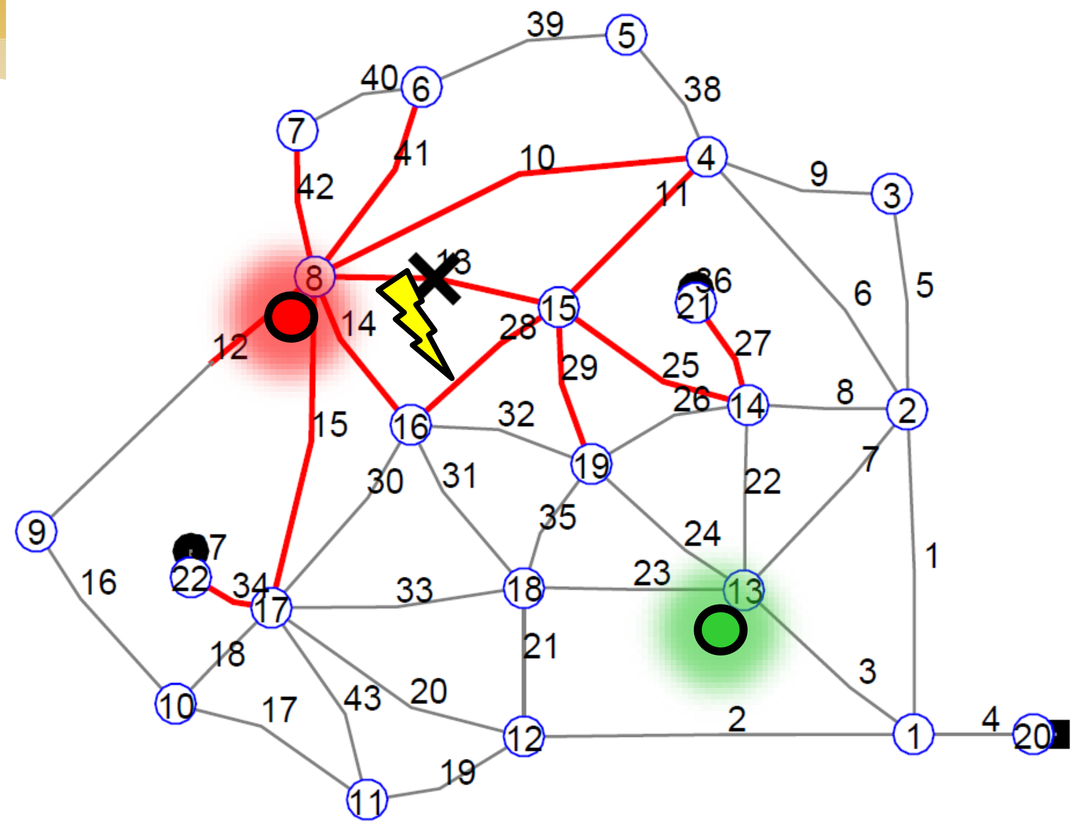
- 22 nodes
- 43 pipes



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

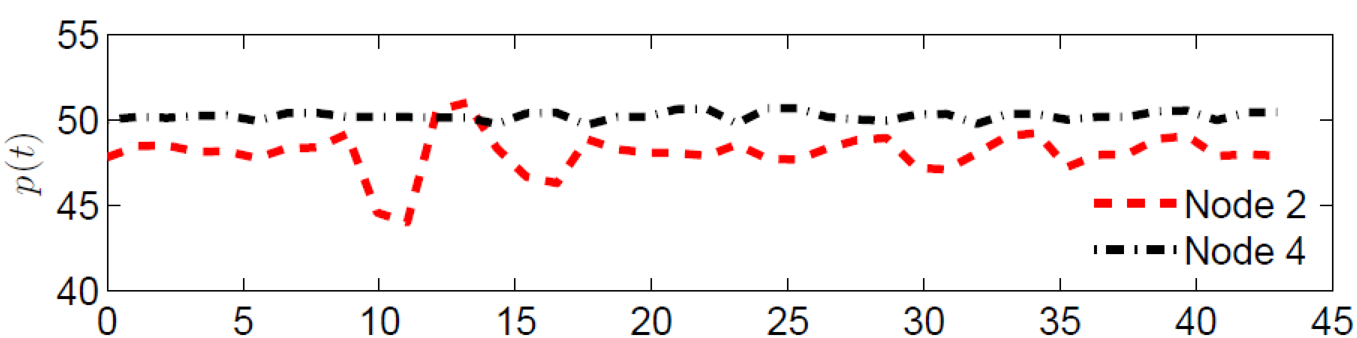
Sensor placement on Anytown network

- 22 nodes
- 43 pipes



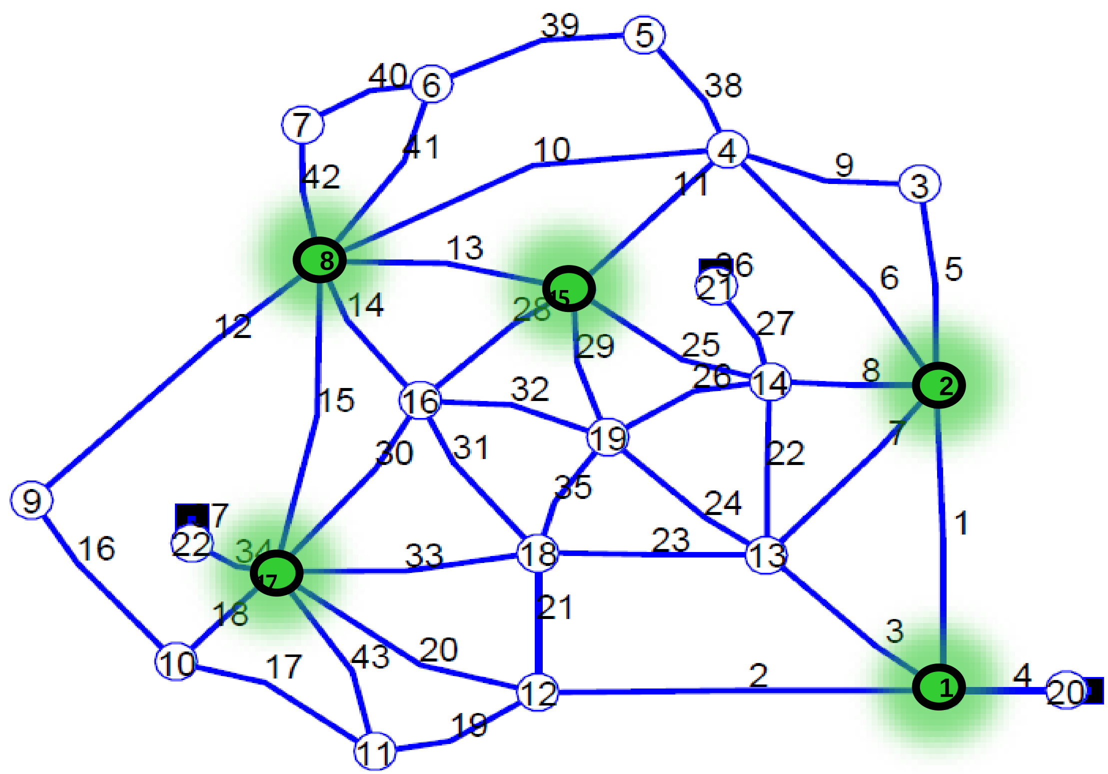
- **Event:** pipe failure
- **Response:** sensing

Pressure



Sensor placement for complete detection

- Minimum set cover



FORCES
FOUNDATIONS OF RESILIENT
CYBER-PHYSICAL SYSTEMS

Attacker – Defender game

Players:

- Defender: sensing over nodes
- Attacker: interdicting pipes

Rules:

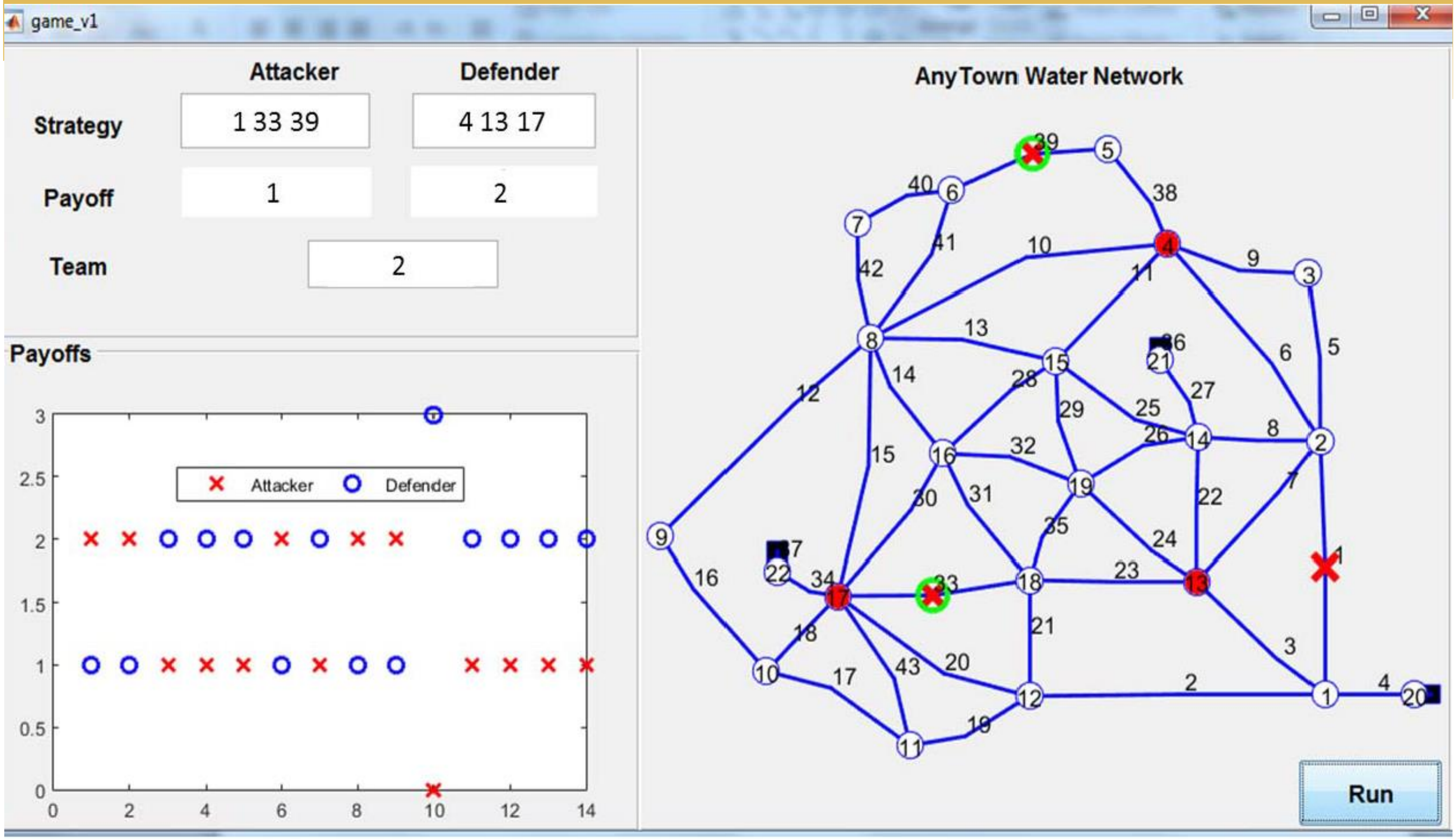
- A sensor can detect an attack within a range of 1.8 [mi]
- Defender can sense 3 nodes
- Attacker can attack 3 pipes
- Players play simultaneously
- Utility of the defender: #detections
- Utility of the attacker: #attacks - #detections

Objective:

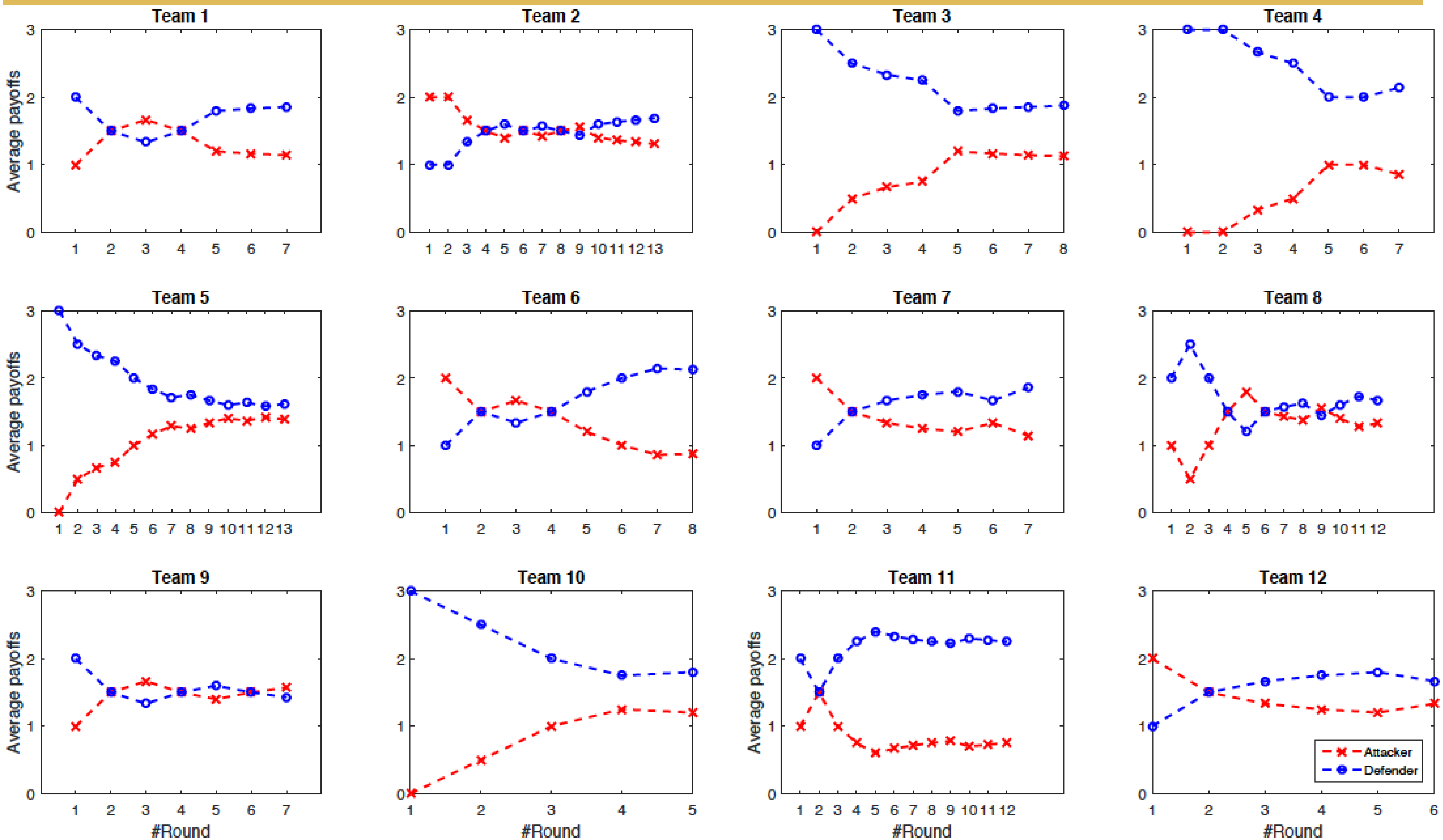
- Maximize individual utility

FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Game interface



Results: Learning via repeated play



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Attackers – Defenders team game

Players:

- Team of Attackers: interdicting pipes
- Team of Defenders: sensing over nodes

Information and Actions:

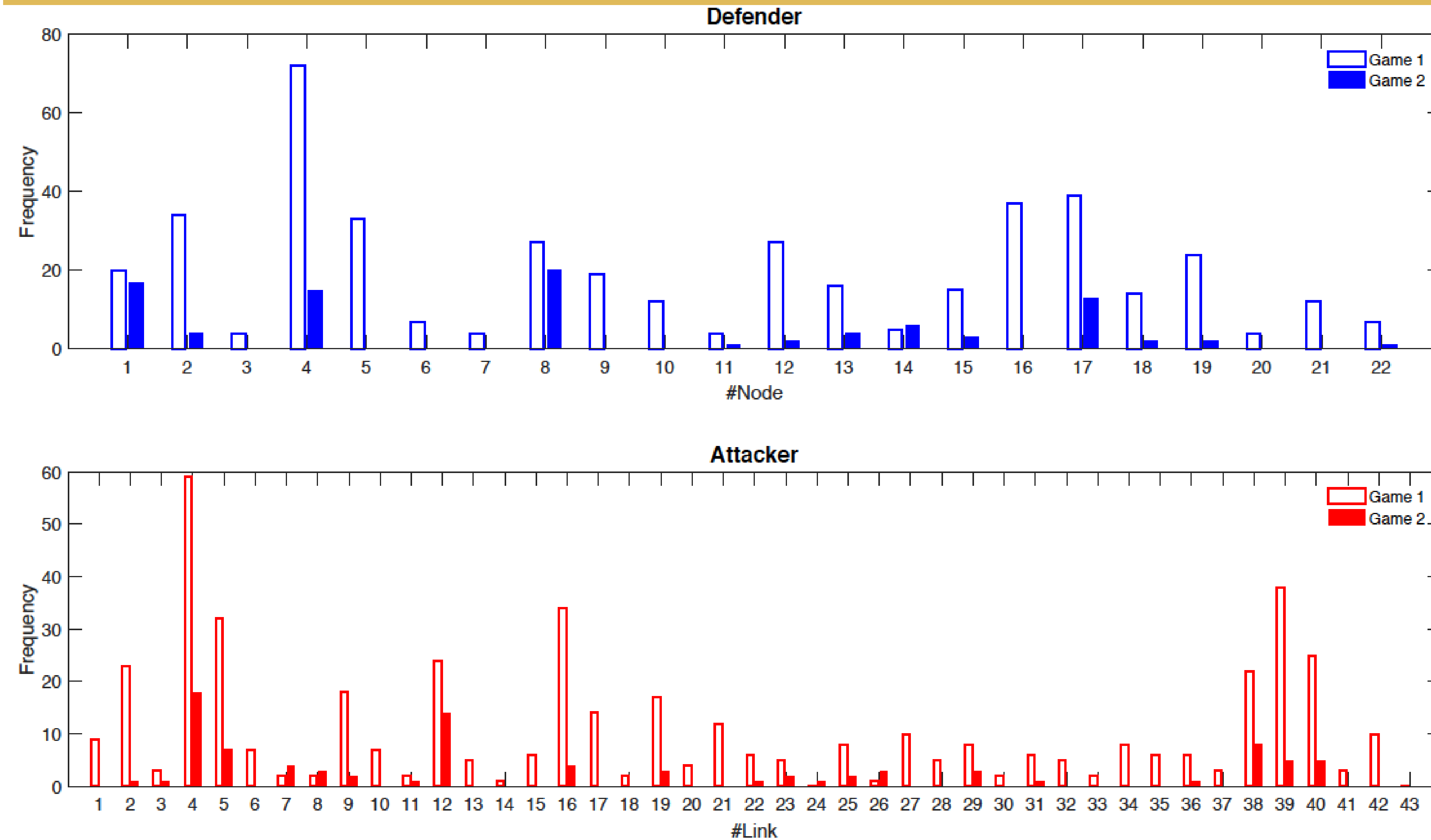
- A sensor can detect an attack within a range of 1.8 [mi]
- Each attacker can attack 3 pipes
- Each defender can sense 3 nodes
- Each attack is paired up against each defense strategy

Payoffs:

- Utility of the attacker: AVERAGE(#attacks - #detections)
- Utility of the defender: AVERAGE(#detections)
- Maximize average utility

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Results: Exploration vs Exploitation



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Student quotes

Isaac Guerrero ‘19

- “This is the first time I’ve been exposed to optimization and game theory. It was interesting to see firsthand the varying strategies people have developed and tested, and compare my own strategies. It was even interesting to see which of my theories were unsuccessful.”

Alexander Lynch ‘19

- “[The module] was fun and really exhilarating. I actually learned a decent amount from the class. Initially, I focused more on the attack side rather than the defense – which I think is the harder part personally.”
- “My favorite part of the module was getting super radical at the end. By the

Bridget Bassi ‘17

- “I chose a systems core at the beginning of this year. I was looking for something a little bit different than the traditional civil engineering route – I’m particularly excited to explore data sets, analyze them, and also delve into the real world applications that associated with civil engineering.”
- “Listening to Professor Amin’s research was very interesting – it mostly struck me because of how applicable it is in a real-world scenario using strategies such math, graph and game theory. It helps to have a greater understanding of everyday instances and everyday networks.”