Protecting Cyber Physical Systems Using A Game-Theoretical Approach

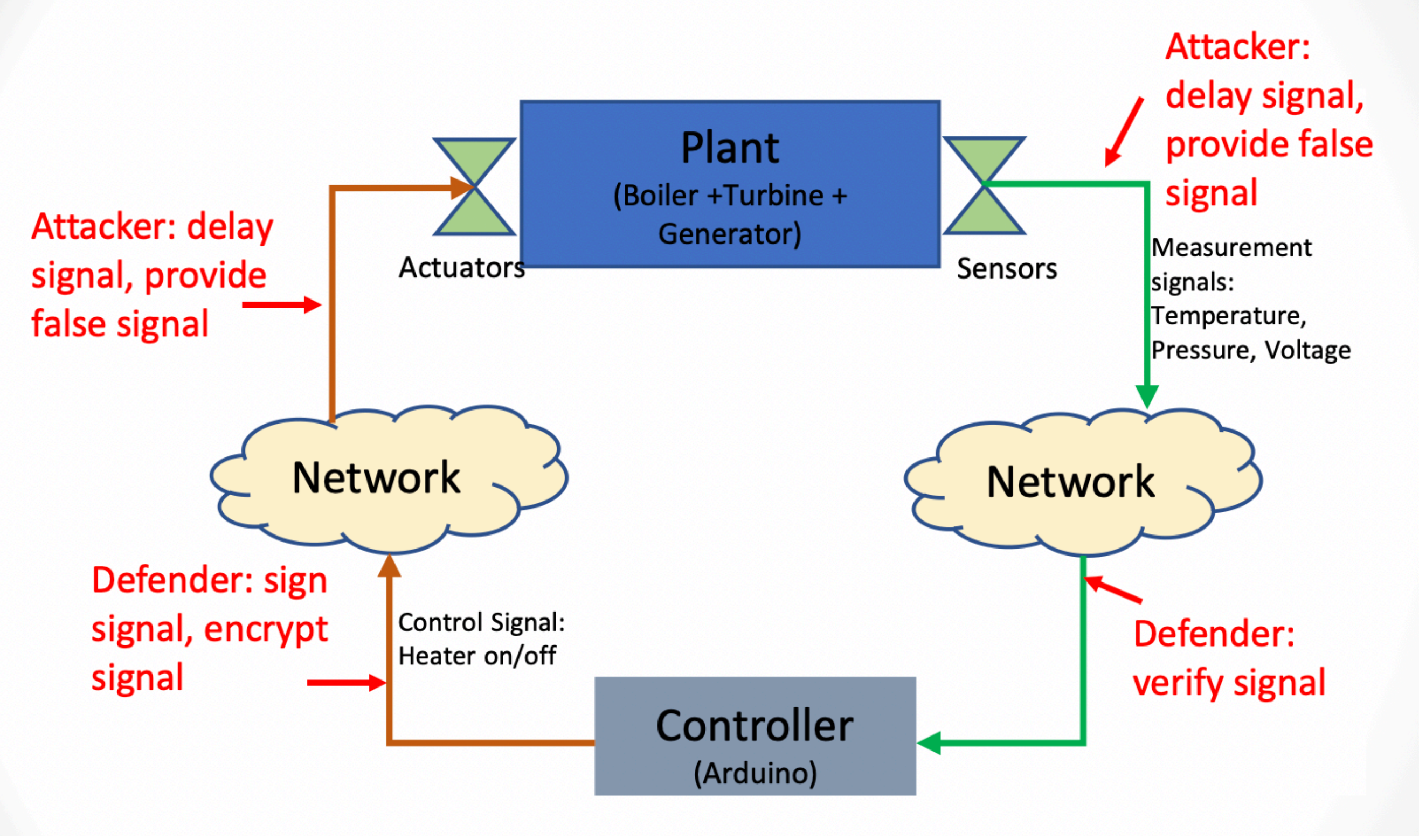
Leander Davis. Mina Guirguis (PI), Texas State University

Motivation

- CPS (Cyber Physical Systems) are now a big part of our everyday lives and as time goes on their usage will grow.
- It is necessary to protect CPS against cyber attacks

Challenges

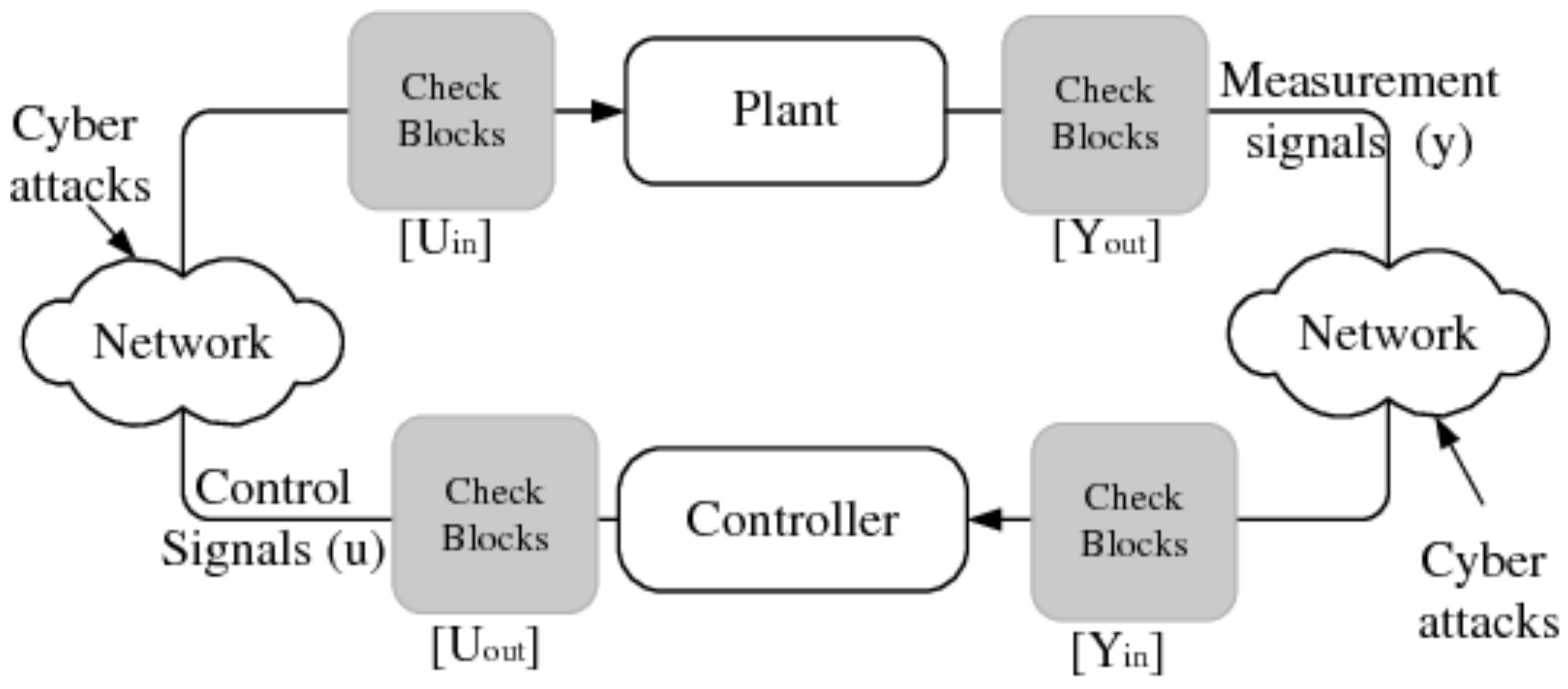
- Complex systems, with real-time and energy constraints widens the malicious opportunities
- Reliance on wireless technology that can be easily jammed and interfered with
- Understanding the interaction between the attacker and defender strategies
- Transitioning from theoretical to implementation (using the CPS test bed)


Attacker: delay signal, provide false signal
Actuators
Plant
(Boiler +Turbine + Generator)
Sensors
Attacker: delay signal, provide false signal
Measurement signals: Temperature, Pressure, Voltage
Network
Network
Defender: sign signal, encrypt signal
Control Signal: Heater on/off
Controller
(Arduino)
Defender: verify signal

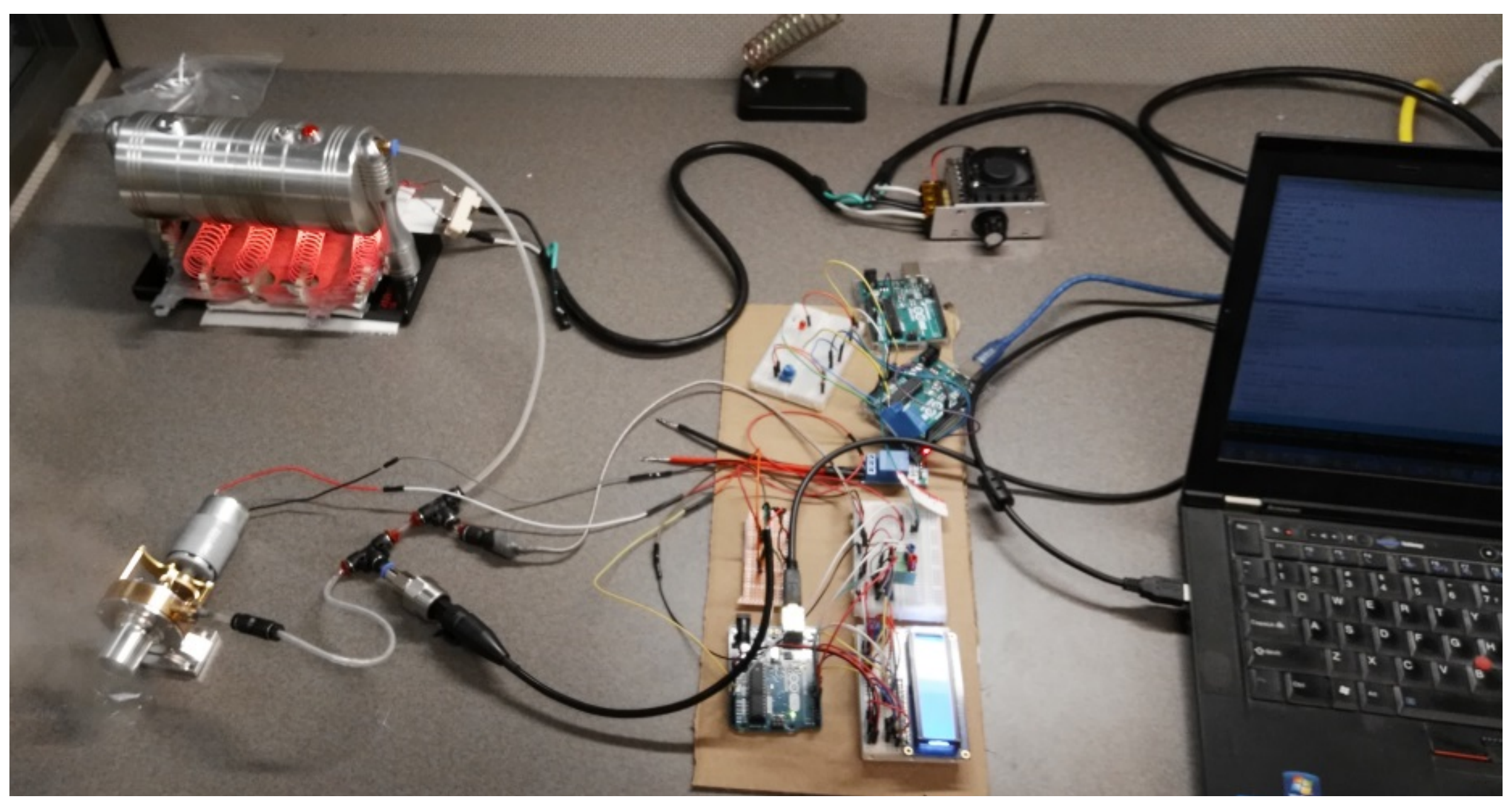
Vulnerable CPS

Methodology

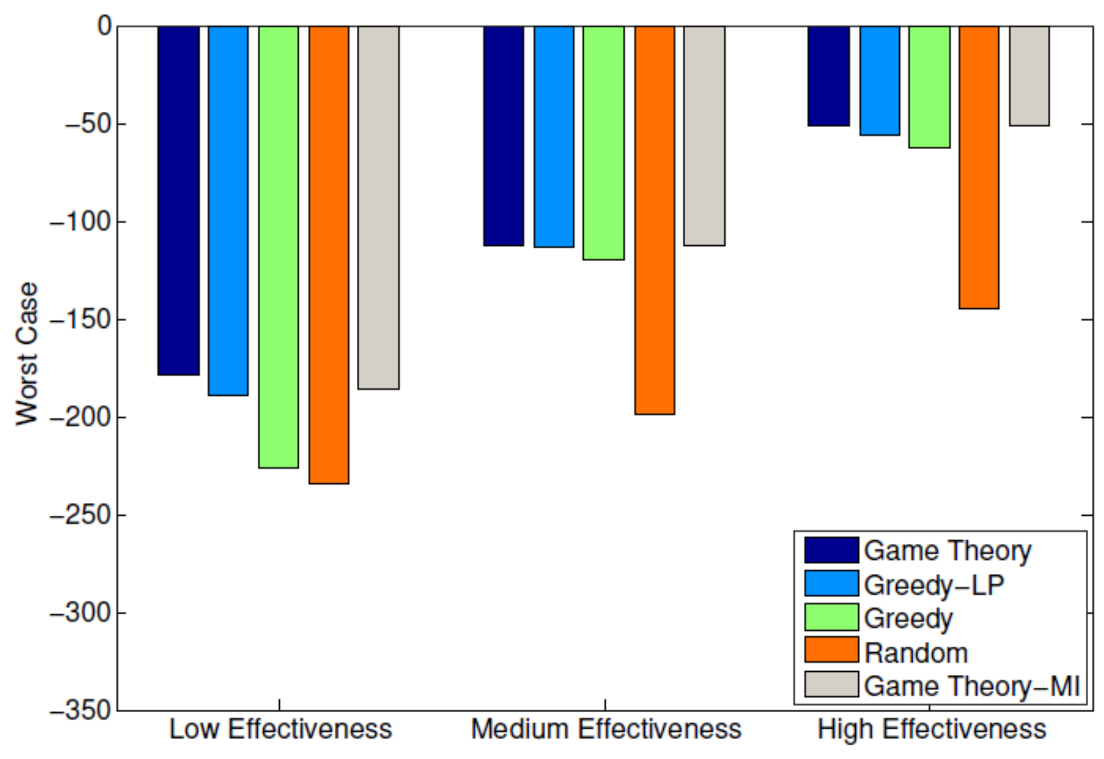
- Maximin Q-Learning
  - Game Theoretic version of Q-Learning algorithm
- 2 players: attacker and defender
  - Attacker decides which signals to attack
  - Defender decides which check blocks to assign
- The curse of dimensionality
  - State and action spaces are exponential in number of signals to attack and check blocks to assign
- CPS test bed
  - Physical test bed for policies



Protected CPS



CPS Test Bed



Defensive Policy Effectiveness

Impact

Broader Impact

Protection of CPS, such as our power grid, delivery drones and smart signs, is important as CPS are becoming the hidden gears of modern life.

Educational Impact

Any decision involving multiple agents with a large state space can benefit from using Maximin Q-Learning.

Potential Impact

The use of Maximin Q-Learning to develop signal security policies for CPS has the to potential to provide better protection for our CPS.