A FRAMEWORK FOR RESILIENCE AND SECURITY IN CYBER-PHYSICAL SYSTEMS

BHASKAR RAMASUBRAMANIAN, POSTDOCTORAL RESEARCHER, NETWORK SECURITY LAB

MOTIVATION

- CPS: physical parts + comm. channels + algorithms
- Found across scales, sizes, geographies
- Tight integration ⇒ vulnerable to attacks
- Compromised CPS can disrupt everyday life
- Strategies for benign env. fail in presence of adversary



CHALLENGES

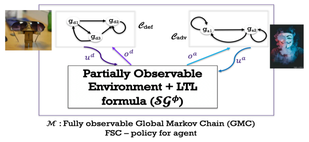
- Translating security into CPS models
- Modeling interaction of CPS with adversary
- Characteristics of environment and specifications
  - states may not be fully observable
  - different strategies for discrete and continuous environments
  - satisfaction of time-critical properties

OPPORTUNITIES

- **Formal Methods**: specify desired system objective
- **Game Theory**: interaction of CPS with adversary
- **Optimization**: efficient protocols and algorithms to ensure resilience to adversary
- **Inertia of physical system**: managing time-critical specifications and recovery from attack

- **MODEL:** CPS - adversary interaction modeled as a *zero-sum leader-follower stochastic game*
- **GOAL:** Determine CPS inputs to max. probability of satisfying temporal goal ϕ under any adversary input
- **SOLUTION APPROACH:** Optimal solution is equilibrium of CPS - adversary Stackelberg game

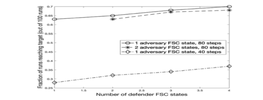
I. PARTIALLY OBSERVABLE ENVIRONMENTS



$\mathcal{M}$: Fully observable Global Markov Chain (GMC)
FSC – policy for agent

goal: **G F green** ∧ **G** ¬ **red**
$\mathcal{O}_{def} = \mathcal{O}_{adv}$ = {correct, wrong}
assume: $|G_{def}| \geq |G_{adv}|$

s_0	s_1	s_2	s_3	s_4
s_5	s_6	s_7	s_8	s_9
s_{10}	s_{11}	s_{12}	s_{13}	s_{14}
s_{15}	s_{16}	s_{17}	s_{18}	s_{19}



1. For fixed $|G_{adv}|$, more runs reach goal for higher $|G_{def}|$
2. For fixed $|G_{def}|$, more runs reach goal for smaller $|G_{adv}|$

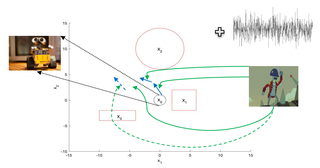
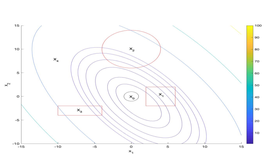
- Partial observability common – e.g. estimate of state from output of a vision sensor, noisy communication channel
- Partial observability ⇒ exact strategies difficult to determine

SOLUTION METHOD

- Desired objective given in **Linear Temporal Logic**
- Use finite state controllers (FSCs) as agents' policies
- FSC + env. + LTL spec = fully observable Markov chain (MC)

1. **THEOREM:** $\mathbb{P}$(satisfying ϕ) = $\mathbb{P}$(reaching certain states in MC). Extends to stationary CPS policies that maximize this probability under any stationary adversary policy
2. **ALGORITHM**: determine candidate FSCs of fixed sizes that ensure LTL satisfaction with nonzero probability
3. **ALGORITHM**: robust linear program to increase size of CPS FSC to improve satisfaction probability

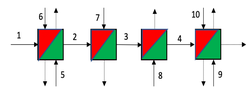
II. CONTINUOUS STATE AND ACTION SPACES

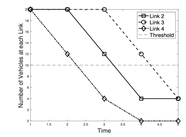
SOLUTION METHOD

- Barrier certificates enable verification of safe behavior
- **Secure Control Barrier Certificates (S-CBC)**: for some defender action, increase in S-CBC value is bounded along system trajectories for any adversary action
- S-CBCs give lower bounds on LTL satisfaction probability in the presence of adversary, over a finite time horizon
- Sum-of-squares optimization to easily compute S-CBC

III. TIME-CRITICAL OBJECTIVES



TIME	Int.1	Int.2	Int.3	Int.4
1	G	R	G	R
2	R	G	R	G
3	G	G	R	G
4	G	G	G	G
5	G	R	G	G



- Adversary can tamper with actuators and clocks of CPS
- Affects perception of correct time for CPS
- Can lead to violation of desired goal

goal: number of cars in links 2, 3, 4 must be < 10 in 5 seconds

SOLUTION METHOD

- Desired objective given in **Metric Temporal Logic**
- Define durational stochastic game to model time between transitions of states due to CPS and adversary actions
- **ALGORITHM**: determine CPS protocol to maximize probability of satisfying specification while being robust to attacks on clocks and actuators of system
- **ROBUSTNESS METRICS**: quantify maximum amounts by which synthesized trajectories can be perturbed in time and space without affecting satisfaction of desired objective

REFERENCES

[1] Ramasubramanian**,** Clark, Bushnell, Poovendran, `*Secure Control under Partial Observability with Temporal Logic Constraints*', Proc. American Control Conference (ACC), 2019.

[2] Ramasubramanian, Niu, Clark, Bushnell, Poovendran, `*Secure Control in Partially Observable Environments to satisfy LTL Specifications*', Submitted.

[3] Niu, Ramasubramanian, Clark, Bushnell, Poovendran, `*LTL Satisfaction in Adversarial Environments using Secure Control Barrier Certificates*', Proc. Conference on Decision and Game Theory for Security (GameSec), 2019.

[4] Niu, Ramasubramanian, Clark, Bushnell, Poovendran, `*Control Synthesis for Cyber-physical Systems to Satisfy Metric Interval Temporal Logic Objectives under Timing and Actuator Attacks*', Proc. International Conference on Cyber-Physical Systems (ICCPS), 2020.

[5] Niu, Ramasubramanian, Clark, Bushnell, Poovendran, `*Robust Satisfaction of Metric Interval Temporal Logic Objectives in Adversarial Environments*', Submitted.

SPONSORS AND TEAM MEMBERS




ELECTRICAL & COMPUTER ENGINEERING
UNIVERSITY of WASHINGTON

ADVISORS: RADHA POOVENDRAN, LINDA BUSHNELL

SPONSORS: OFFICE OF NAVAL RESEARCH, ARMY RESEARCH OFFICE