CRII: CPS: Secure-by-Design Synthesis of Cyber-Physical Systems

Principal Investigator: Andrew Clark
Department of Electrical and Computer Engineering
Worcester Polytechnic Institute aclark@wpi.edu

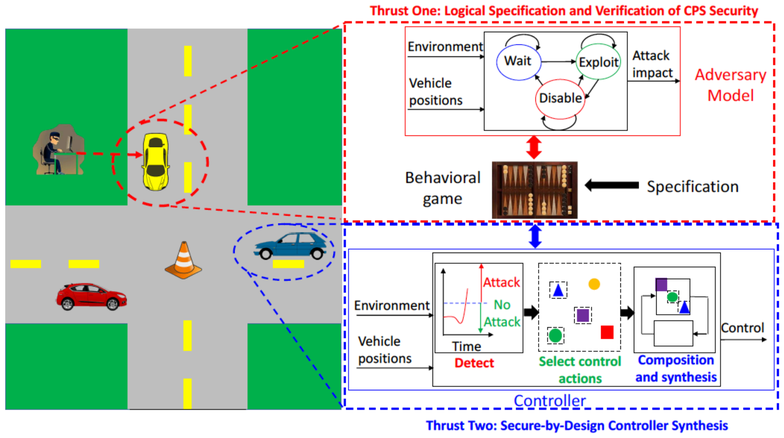
Cyber-Physical System Security

- CPS must satisfy performance and safety requirements (encoded as logical specifications)
- Correct-by-design synthesis: Automatically generate controller based on logical specification
- Performance properties may also be violated by intelligent and malicious attacks (system compromise, false data, DoS,…)

Scientific Questions Addressed

- How to **model the impact** of intelligent attacks on logical specifications of CPS?
- How to **automatically synthesize** control laws that satisfy specifications in the presence of attacks?
- How to **verify** required properties when attacks take place?
- How to jointly ensure resilience to multiple attacks?

Proposed Secure-By-Design Synthesis Framework

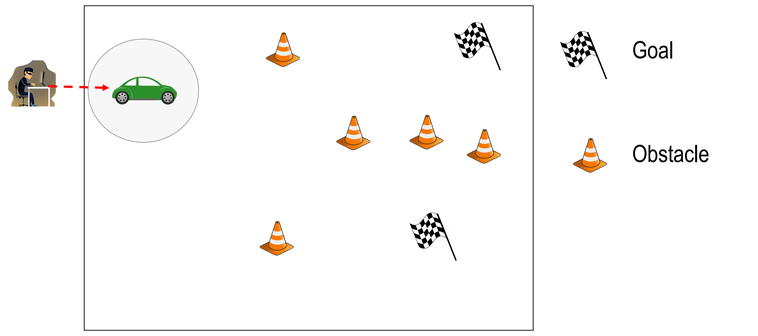


- Formulate logical models that quantify security properties of CPS and impact of adversary actions
- Model interaction between system and adversary via novel N-player simulation games
- Develop control policies based on solutions to games
- Develop methodologies for composing control strategies for resilience to multiple attacks

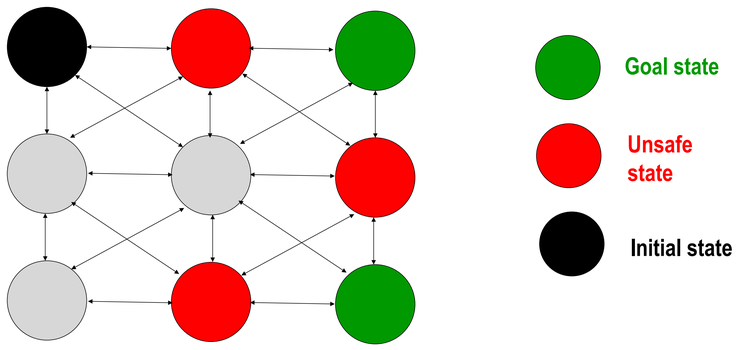
Broader Impact

- Integration into graduate course projects and undergraduate Major Qualifying Projects (MQPs)
- Secure control design Matlab toolboxes
- Implementation, testing, and validation on mobile robot platforms
- High school summer outreach programs

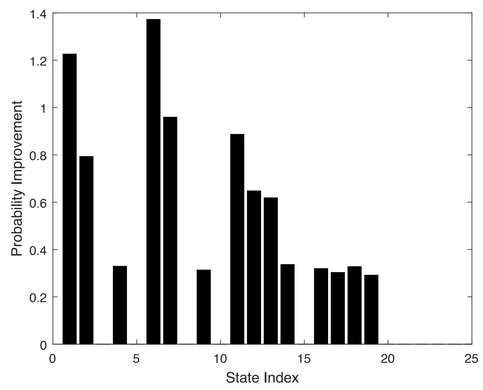
Ensuring Safety and Reachability Under Insider Attacks



- Goal of system: Reach target states infinitely often while avoiding unsafe states (obstacles)
- Adversary can inject **false control inputs** to a subset of actuators in order to thwart system objectives



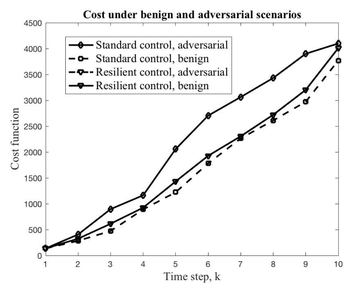
- Model interaction as Competitive Markov Decision Process (CMDP)
- Stackelberg game framework:
  - Control policy selected first
  - Adversary chooses attack strategy based on policy
  - Naturally leads to stochastic control policies
- Proposed computationally efficient algorithms for:
  - Maximizing the probability of satisfying specification
  - Minimizing the rate of constraint violation

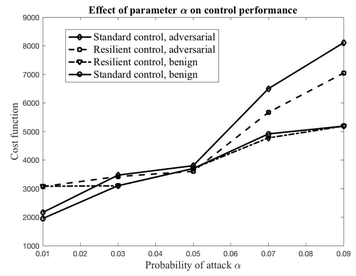


Probability of success and rate of violation are both significantly improved compared to non-resilient policies

Preliminary Work: Control Under False Data Injection Attacks

- Scenario where adversary injects false inputs in order to degrade controller performance
- Example: GPS spoofing in order to misdirect autonomous vehicle
- Preliminary results: Linear Quadratic Gaussian (LQG) control when one or more sensors are compromised
- Formulated two-stage optimization approach
  - First stage: Select a set of feasible control actions
  - Second stage: Select an optimal control action based on received inputs





- Proposed resilient control approach outperforms standard LQG control under attack scenario, comparable performance in benign environment
- Performance improvement is increasing in attack probability

References

[1] L. Niu and A. Clark, "Secure Control Under Linear Temporal Logic Constraints." Submitted to American Control Conference (ACC), 2018.

[2] L. Niu and A. Clark, "Optimal Secure Control with Linear Temporal Logic Constraints." Submitted to IEEE Transactions on Automatic Control (TAC).

[3] A. Clark and L. Niu, "Linear Quadratic Gaussian Control Under False Data Injection Attacks." Submitted to American Control Conference (ACC), 2018.

[4] A. Clark and S. Zonouz, "Cyber-Physical Resilience: Definition and Assessment Metric." Under revision at IEEE Transactions on Smart Grid, 2017.