CPS: CAREER: Formal Synthesis for Provably Correct Cyber-Physical Defense with Asymmetric Information

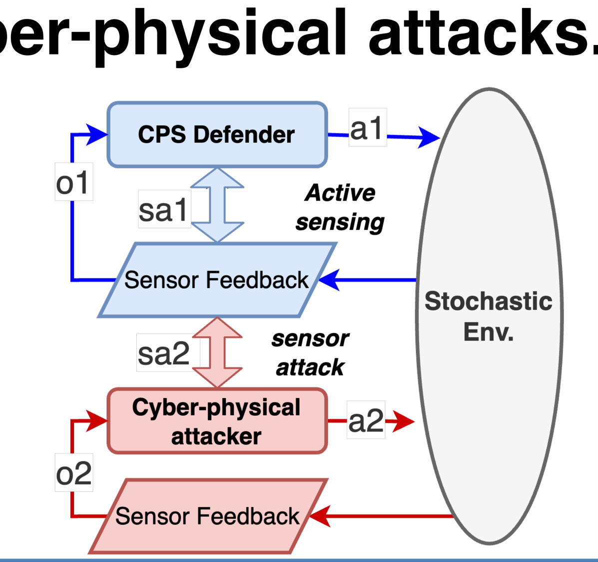
PI: Jie Fu, University of Florida

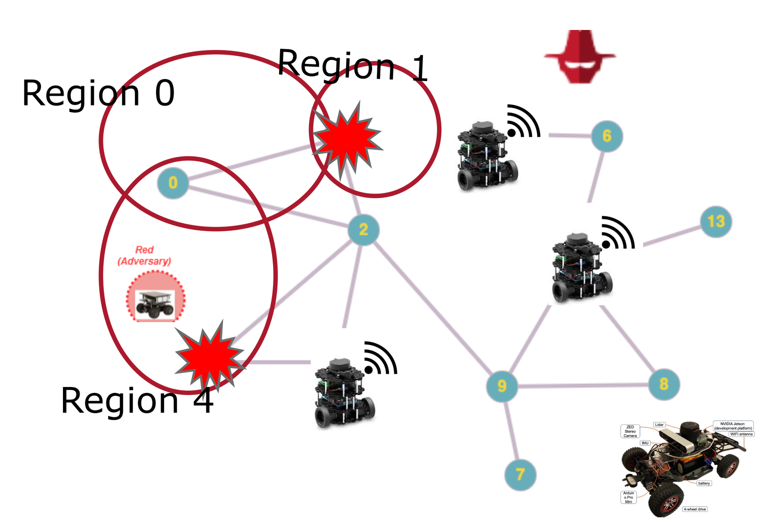
Motivation:

- **Information and knowledge** play a key role in interaction between the CPS defender and attacker.
- Need **assurance** for mission- and safety-critical CPSs.
- Possibility to use **advanced cyber defense with deception** for CPS defense.

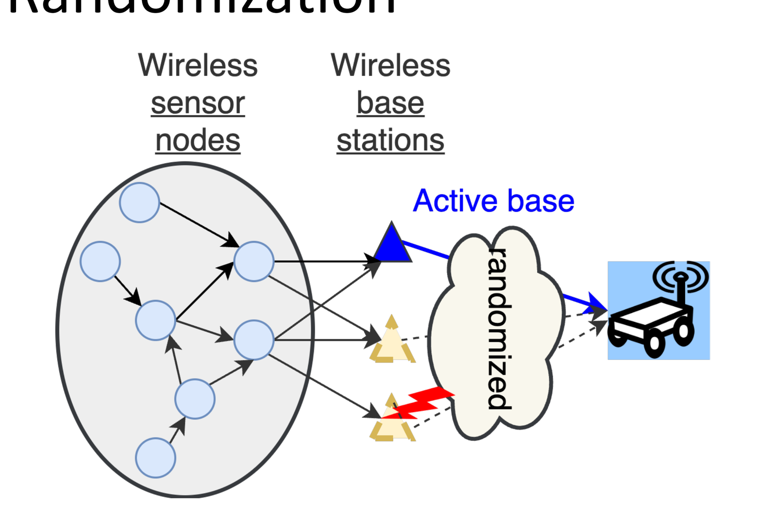
CPS Attack-defend games on graphs:

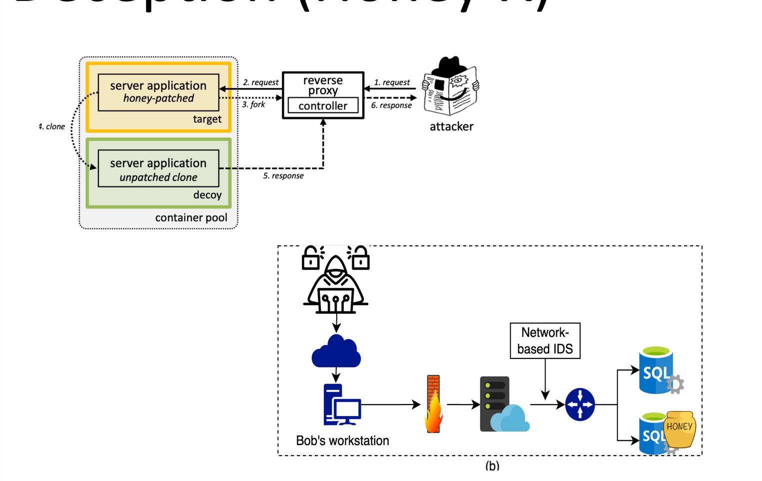
- Games on graphs with partial information $T = (S, A_1 U A_2, P, s_0, O_1, O_2)$
- Missions in temporal logic objective.
- **Asymmetric information**: Sensor randomization, task randomization, honey sensors/robots.
- **Joint perception and control against coordinated cyber-physical attacks.**





Asymmetric information





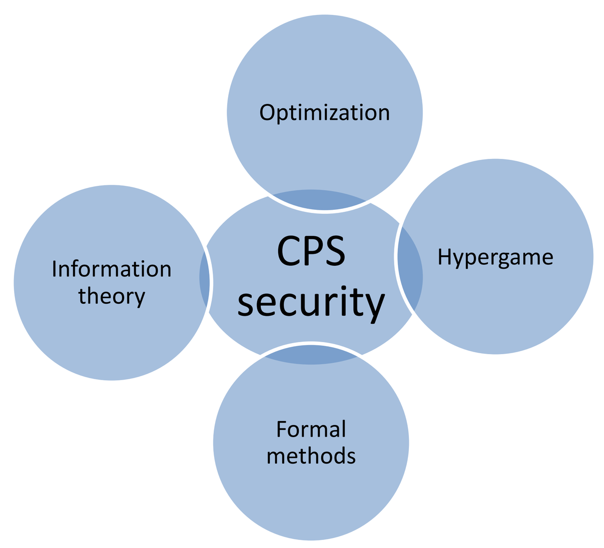
Research thrusts:

Thrust I: imperfect information CPS games and symbiotic defense.

Thrust II: Asymmetric information CPS games.

Thrust III: CPS games against coordinated attackers and preference-aware defense.

Scientific Impact:



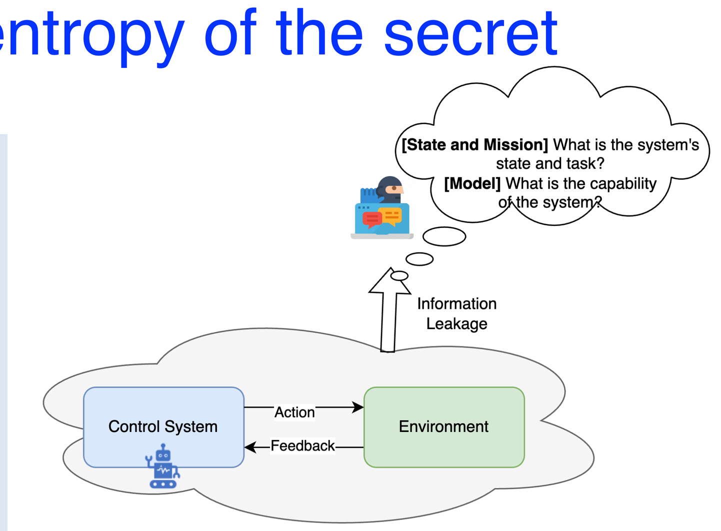
- Bi-level optimization for proactive defense game and adaptive incentive design.
- Hypergame theory for synthesizing CPS deception.
- Information-theory and formal methods for secured- and correct-by-construction.

Key innovation 1: Opacity-by-construction

Maximizing the opacity = Minimize the conditional entropy of the secret

Z: The random variable from the intruder's estimator. (current-state, initial-state, or certain events)

Y: the observations about the system.



$$\text{maximize}_\theta H(Z|Y;\pi_\theta)$$
$$\text{s.t. : } V(s_0, \pi_\theta) \geq \alpha.$$

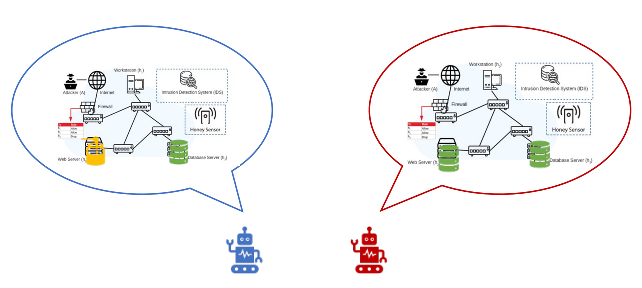
- Opacity in uncontrollable environments.
- Information-theoretic opacity- enforcing control

Key innovation 2: Proactive defense with deception

Defense countermeasures:

$\vec{x}$: Increased attack action cost.
$\vec{y}$: Decoy resource allocation (fictitious rewards)

$M = \langle S, A, P, \nu, \gamma, R_2 \rangle.$ $\quad M_2 = \left\langle S, A, P^{\vec{y}}, \nu, \gamma, R_2^{\vec{x},\vec{y}} \right\rangle.$



Evaluating the attacker's best response for the defender's payoff

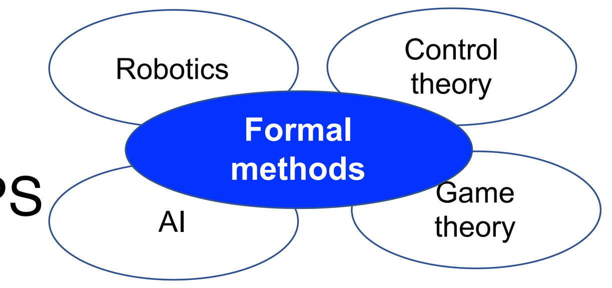
$$\max_{x,y} V_1^{\pi^*}(s_0; y)$$

$$\text{s.t.: } \pi^* \in \arg\max_{\pi} V_2^{\pi}(s_0; x, y)$$

Attacker's best response to the misperceived attack graph.

- Defense synthesis against the best response of the attacker.
- Robust defense synthesis with uncertain attack intention.
- Adaptive defense synthesis against persistent attacks.

Broader Impacts:



- Course development:
  - Formal methods for CPS
- Enhance the security of CPS applications. Provide tools for practitioners to assess the safety and security issues.
- Project-based curriculum to train students of security practice.

References:

1. H. Ma, S. Han, C. Kamhoua, and J. Fu, "Optimal Resource Allocation for Proactive Defense with Deception in Probabilistic Attack Graphs," in Decision and Game Theory for Security, Springer Nature Switzerland, 2023, pp. 215–233.
2. H. Ma, S. Han, C. A. Kamhoua, and J. Fu, "Optimizing Sensor Allocation Against Attackers With Uncertain Intentions: A Worst-Case Regret Minimization Approach," IEEE Control Systems Letters, vol. 7, pp. 2863–2868, 2023.
3. H. Ma, S. Han, A. Hemida, C. Kamhoua, and J. Fu, "Adaptive Incentive Design for Markov Decision Processes with Unknown Rewards," presented at the International Joint Conference on Artificial Intelligence, Under Review 2024.
4. S. Udupa, H. Rahmani, and J. Fu, "Opacity-enforcing active perception and control against eavesdropping attacks ⋆," in Decision and Game Theory for Security, Avignon, France: Springer, Oct. 2023.
5. C. Shi, A. N. Kulkarni, H. Rahmani, and J. Fu, "Synthesis of Opacity-Enforcing Winning Strategies Against Colluded Opponent," in IEEE Conference on Decision and Control, 2023.
6. C. Shi, Y. Bu, and J. Fu, "Information-Theoretic Opacity-Enforcement in Markov Decision Processes," presented at the International Joint Conference on Artificial Intelligence, Under review 2024.

Award #2144113