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

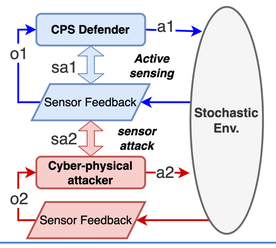
PI: Jie Fu, University of Florida

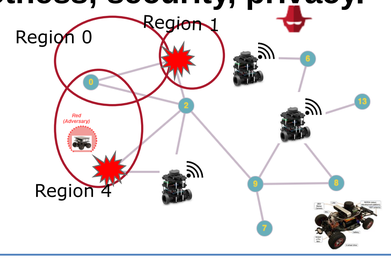
## Motivation:

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

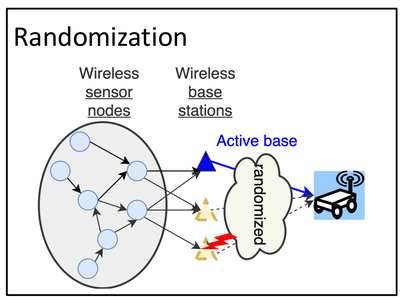
## CPS Attack-defend games on graphs:

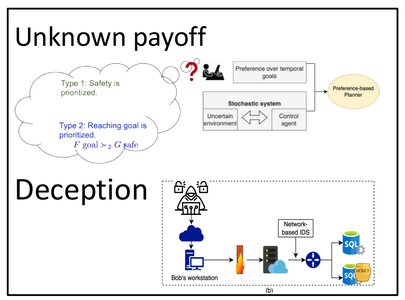
- Games on graphs with partial information $T = (S, A_1 U A_2, P, s_0, O_1, O_2)$
- Missions in temporal logic objective.
- **Asymmetric information**: partial observations, incomplete knowledge about the interaction.
- **Joint perception and control against cyber-physical attacks: correctness, security, privacy.**




## Asymmetric information



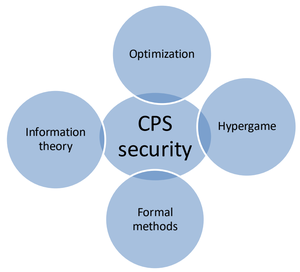

## Research thrusts:

**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.**

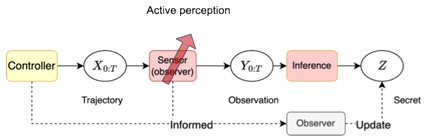
## Scientific Impact:




- Hypergame theory for synthesizing CPS deception.
- Bi-level optimization for proactive defense game and adaptive incentive design.
- Information-theory and formal methods for mission-privacy and security.

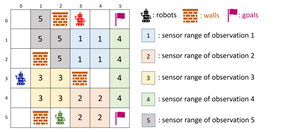
## Key innovation 1: Active perception for fault detection and prediction [7,10]

Motivation: Early detection of abnormal behaviors in dynamical systems using strategic sensor queries.




$$\min_{\pi \in \Pi} H(S_0 | Y_{0:T}; M_\pi),$$

- Improve inference accuracy despite incorrect prior.



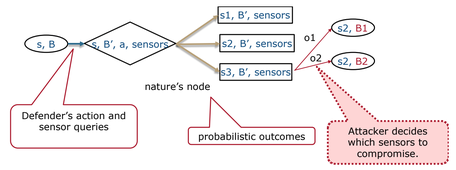




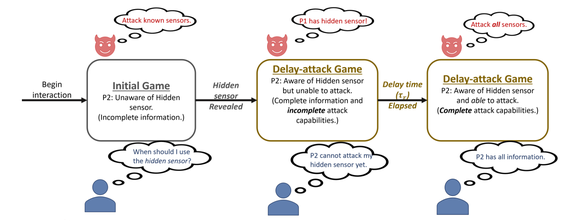
- Maximizing information leakage for adversarial intent recognition and abnormality detection.
- (Ongoing) fault prognosis with noisy sensors.

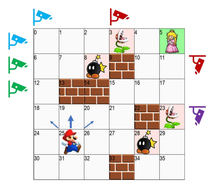
## Key innovation 2: Reactive sensor revealing for mitigating CPS-attack

*Defense with deception to sensor attack:*




Two-player game: Joint control and active perception against sensor attacks.



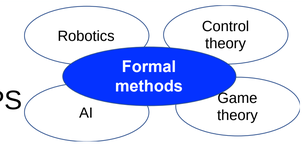
- S0-Green, S1-Red, S2-Blue, S3-Purple.
Initially, sensors S1 and S3 are hidden.

| Setup ($\tau$) | Deceptive Winning Initial States | VoD |
|---|---|---|
| Case 1 (-) | [4, 10, 11, 16, 17, 5] | 0 |
| Case 2 (0) | [4, 10, 11, 16, 17, 5] | 0 |
| Case 2 (1) | 15, 20, [4, 10, 11, 16, 17, 5] | 0.105 |
| Case 2 (2) | 21, 27, 32, 34, 15, 20, [4, 10, 11, 16, 17, 5] | 0.315 |
| Case 2 (3) | 26, 31, 21, 27, 32, 34, 15, 20, [4, 10, 11, 16, 17, 5] | 0.421 |

Sensor revealing: *"When to query which hidden sensor to ensure satisfying a temporal logic task despite sensor 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.

**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, 2024.*
7. *C. Shi, S. Han, M. Dorothy, and J. Fu, "Active Perception With Initial-State Uncertainty: A Policy Gradient Method," IEEE Control Systems Letters, vol. 8, pp. 3147–3152, 2024, doi: 10.1109/LCSYS.2024.3513896.*
8. *S. Udupa and J. Fu, "Planning with Probabilistic Opacity and Transparency: A Computational Model of Opaque/Transparent Observations," presented at the IEEE Conference on Decision and Control, 2024.*
9. *S. Udupa, A. Hemida, C. A. Kamhoua, and J. Fu, "Reactive Synthesis of Sensor Revealing Strategies in Hypergames on Graphs," Dec. 02, 2024, arXiv: arXiv:2412.01975. doi: 10.48550/arXiv.2412.01975. under review at Automatica, 2025.*
10. *S. Udupa, C. Shi, and J. Fu, "Synthesis of Dynamic Masks for Information-Theoretic Opacity in Stochastic Systems," 16th ACM/IEEE International Conference on Cyber-Physical Systems, 2025.*

Award #2144113