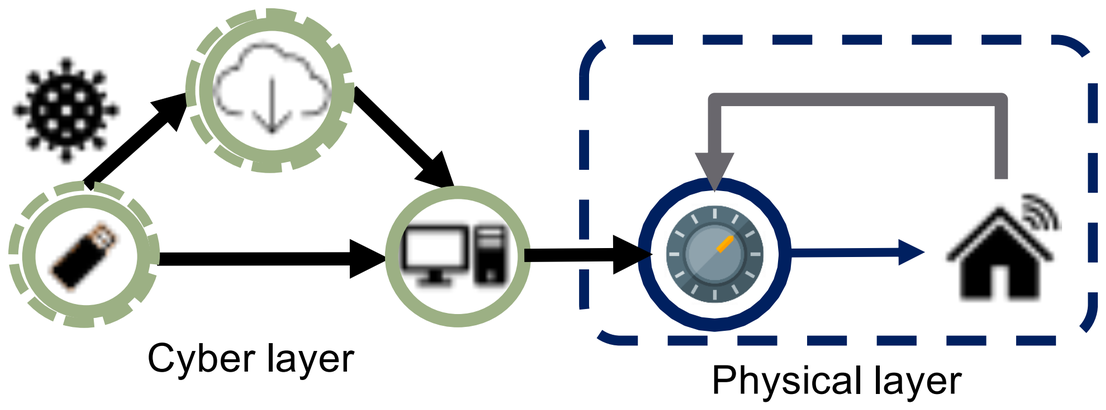
SaTC: CORE: SMALL: Data-driven Attack and Defense Modeling for Cyber-physical Systems (CPS)

PI: Shaunak D. Bopardikar, Michigan State University

https://github.com/sandeepbanik/Data-Driven-Resilient-Systems

- CPS are vulnerable to wide range of attack progressions
- Red team: Finds new system vulnerabilities
- Blue team: Uses this knowledge to allocate defenses
- **Objective: A data-driven purple teaming framework for enhancing CPS security**



Key challenges:

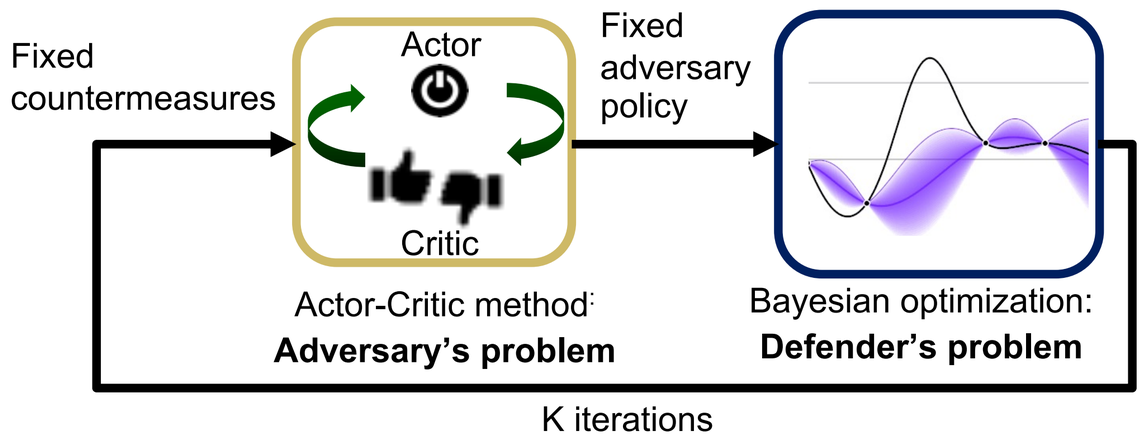
- Coupled security requirements between cyber and physical layers
- Continuous search to account for newer vulnerabilities
- Hybrid state spaces with high computational complexity
- Dynamic nature of cyber networks

Scientific impact:

- Systematic deployment of countermeasures for resource constrained CPS
- Quantifying fundamental limits on performance loss
- Security principles for Learning-enabled CPS
- Increased readiness to zero-day attacks

Solution:

- Automated strategies to characterize attacker intent using **reinforcement learning**
- Integrated defense to guide countermeasures using **game-theoretic methods**
- Realistic validations in **intelligent buildings** applications



Broader Impact on Society

- Critical systems -- power grids, energy distribution
- Temperature control in vaccine distribution facilities
- Secure autonomous vehicle operations

Broader Impact – Education and Outreach

- Interactive attacker-defender games for pre-college STEM aspirants
- Curriculum enrichment for the PI's graduate course on Game theory at MSU.
- Share findings with vaccine distributors (e.g., hospitals)

Broader impact and broader participation

- Include at least one underrepresented student in project demos
- Serve as mentor to at least one schoolteacher as part of the NSF RET at MSU
- Collaborate with Pacific Northwest National Lab