Building Intelligence in Cyber-Physical Systems

CAREER: Towards Secured and Efficient Energy-based Critical Infrastructure

PI: Wei Yu; Towson University

Challenge

- CPS inherently operates under the presence of various uncertainties
- While machine learning has receiving great success in a number of areas, leveraging it in CPS face significant challenges -- considering exceptional requirements of CPS

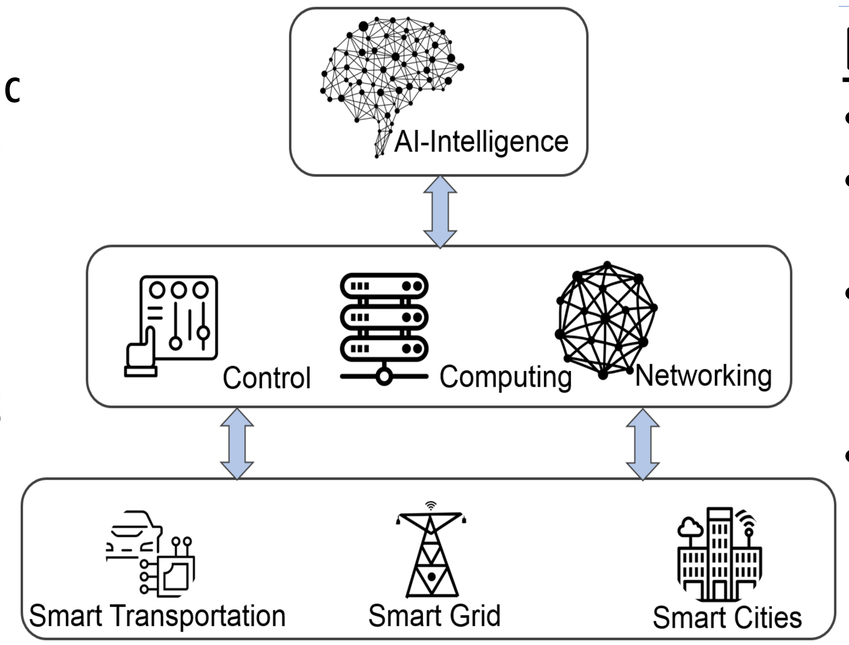
Solution

- Design deep learning architectures anc algorithms to meet strict performance requirements in CPS
- Qualify the impacts and uncertainties raised by attacks that target deep learning algorithms and models in CPS
- Design techniques to improve the security resilience of deep learning algorithms and models in CPS

Award #: CNS-1350145; 09/2014 – 08/2021

Scientific Impact

- Characterize information flows and attacks with different strategies in CPS
- Study the good, the bad, and ugly use of machine learning in CPS
- Design a framework for applying reinforcement learning to improve the performance of CPS
- Design a modeling framework to forecast timescale machine traffic dynamics and investigate the impact of data integrity threats
- Develop deep learning based schemes for predicting smart grid energy consumption and parking lots utilization



Broader Impact

- Publish 10+ research papers
- Train 5+ graduate and 2 undergraduate students
- Integrate research results into two graduate courses (security and networking)
- Lead two special issues in IEEE Internet of Things Journals ("AI-Enable Internet of Dependable and Controllable Things" and "Security and Privacy in Cyber-Physical Systems")