CPS: Medium: Secure Constrained Machine Learning for Critical Infrastructure CPS

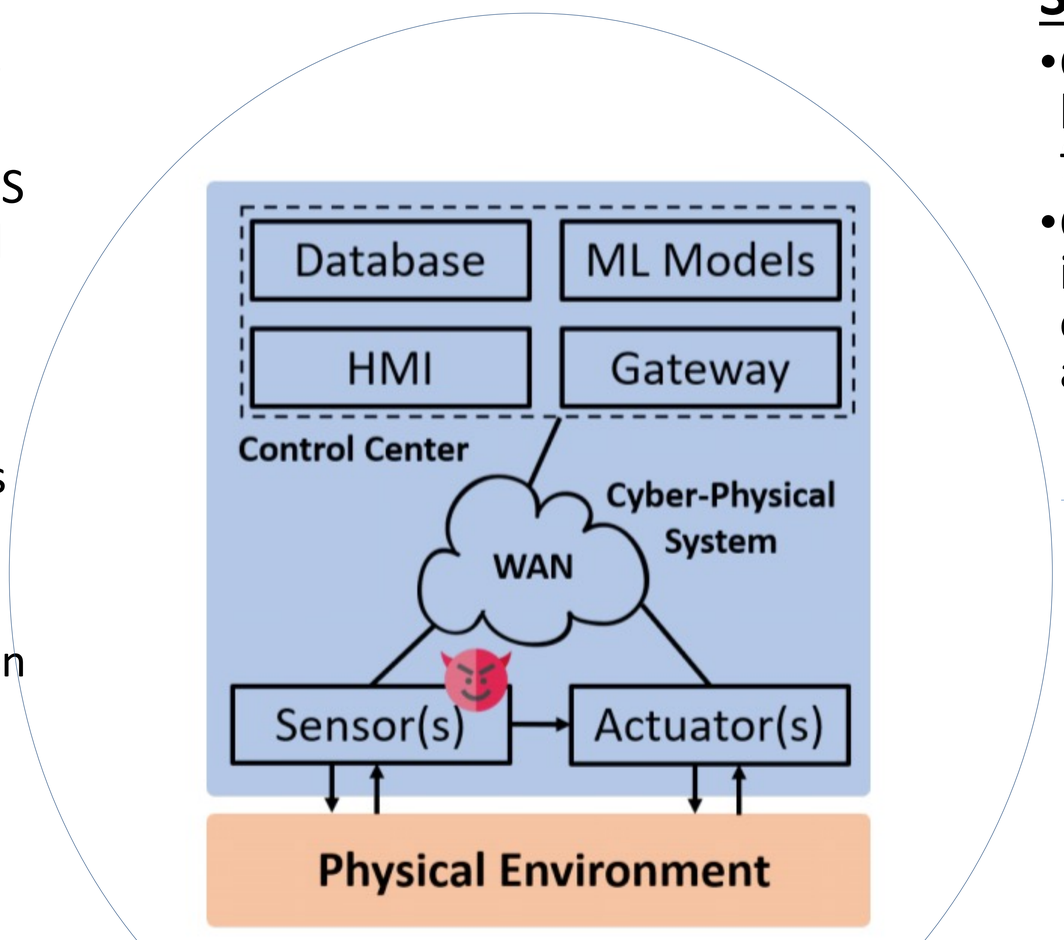
Award # 2038922; Start Date 02/01/2022; J. Sun, H. Qi, K. Tomsovic & L. Han, University of Tennessee

Challenge:

- Lack of threat model, vulnerability assessment, and attack mitigation for machine learning used in CI-CPS subject to physical and topological constraints
- Lack of framework for secure machine learning from ground up taking into account the constraints

Solution:

- Novel watermarking-based mitigation for adversarial attacks on CI-CPS
- Multi-level contrastive learning with local consistency for self-supervised representation learning in the representation module
- Forecast correlations-based constraints applied to deep learning models for electric load and traffic forecasting that flag malicious input data



Machine Learning-assisted CPS

Scientific Impact:

- Contributes to the knowledge base of secure machine learning for CI-CPS
- Can be applied to all complex interconnected CI-CPS including oil and natural gas, water, energy, and transportation systems

Broader Impact:

- Critical infrastructures provide for people's basic needs; their security and reliability are of paramount importance
- Educational plan and outreach activities include involving women and URMs and high-school students in research