2021 NSF CYBER-PHYSICAL SYSTEMS PRINCIPAL INVESTIGATORS' MEETING

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

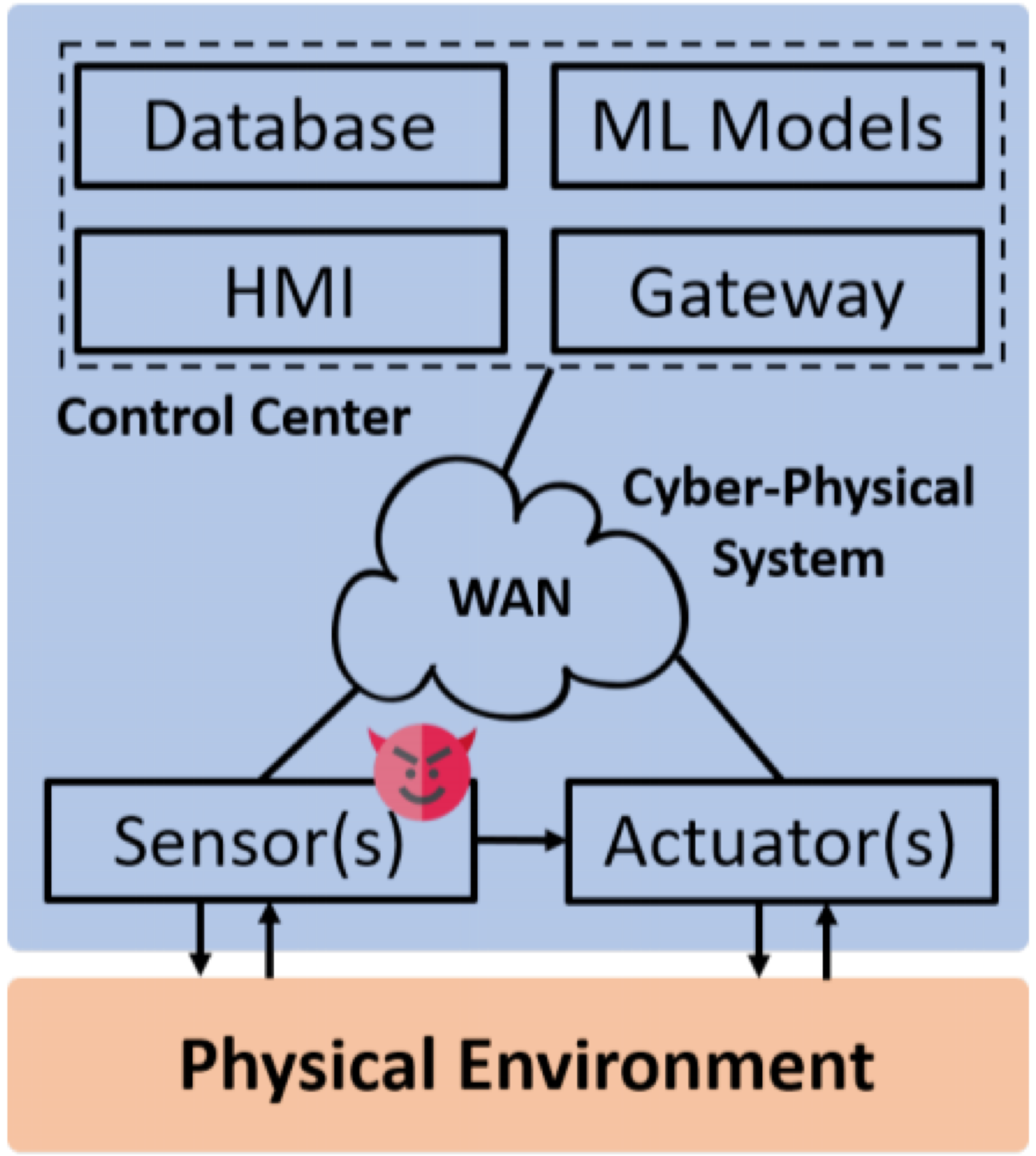
Award # 2038922 **Start date 02/01/2021** **University of Tennessee**

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 gound up taking into account the constraints

Solution:

- Novel adversarial machine learning attacks incorporating the constraints and random padding-based mitigation
- Novel data-representation-model-task association framework for secure machine learning from ground up based on variation Dirichlet network



Machine learning-assisted CPS

Scientific Impact:

- Contributes to the knowledge base of secure machine learning for CI-CPS
- Can be applied to all large 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