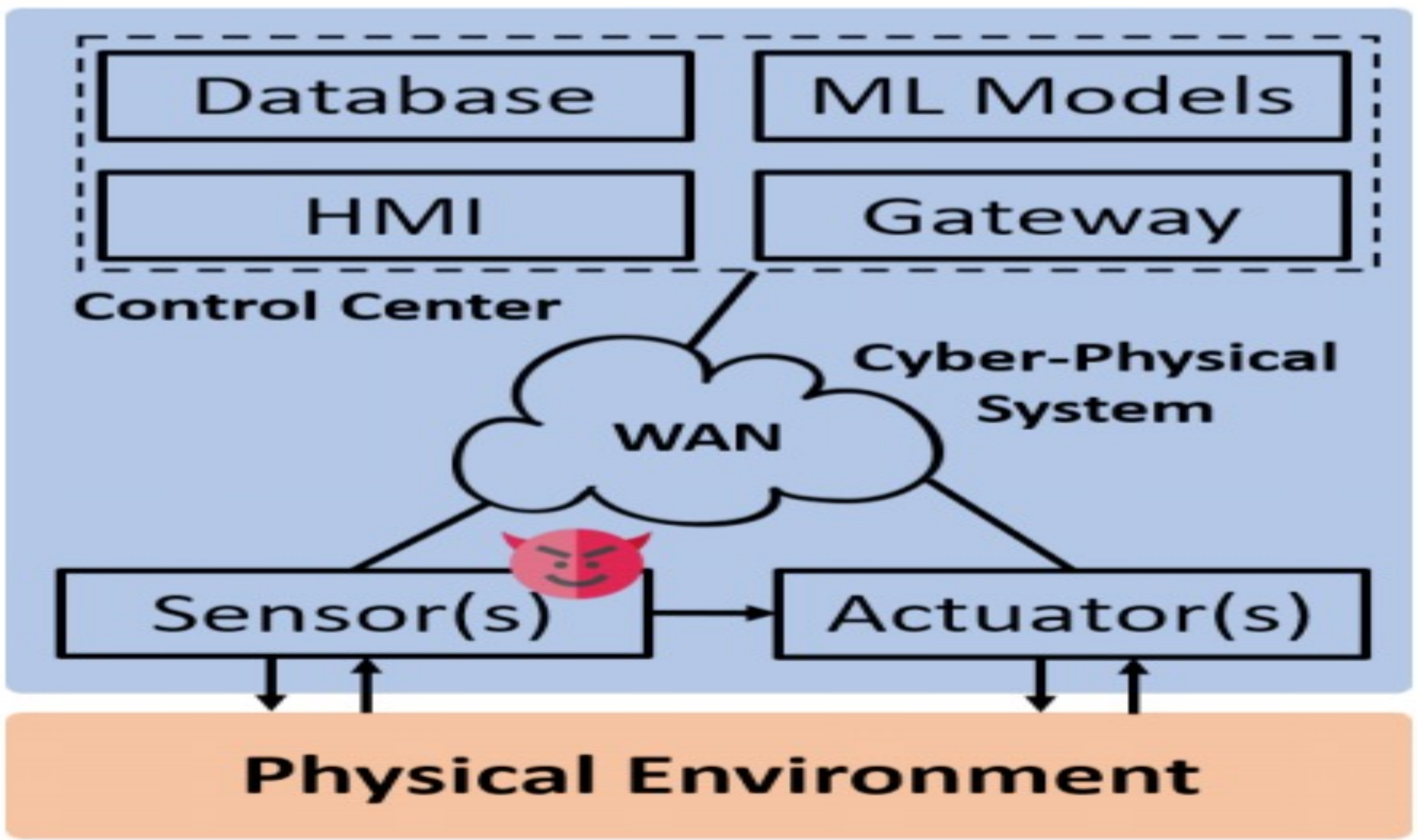
CPS: Medium: Secure Constrained Machine Learning for Critical Infrastructure CPS

PI: Jinyuan Stella Sun; Co-Pis: Hairong Qi, Kevin Tomsovic, Lee 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

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

Solution:

- Developed new ConAML attacks against traffic sign recognition systems.
- Tested and improved a new, more general countermeasure based on model watermarking
- Investigated security analysis using a GNN framework - the GNN model incorporates the network connection and neighboring nodes' influence for the assessment.

Impact on Society:

- Critical infrastructures provide for people's basic needs; their security and reliability are of paramount importance

Education&Outreach:

- Educational plan and outreach activities include involving women and URMs and high-school students in research

Quantifying Impact:

- Strengthening the security posture of CI-CPS reduces the cost of cyber attacks which exceeds $1 Trillion for the power grid alone

Start Date 02/01/2022

Award ID#: 2038922