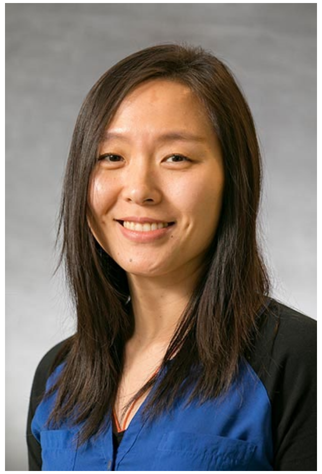


Stella Sun Personal Info

- **Associate Professor in Cybersecurity**
- **Research Interests: cyber-physical security, machine learning security, mobile system security, network security**
- **jysun@utk.edu**

2020-2021 Research Projects

- Secure Constrained Machine Learning for Critical Infrastructure CPS (NSF, with Hairong Qi and Kevin Tomsovic)
- Watching Grid Infrastructure Stealthily via Proxies (DOE, with Fran Li and Kevin Tomsovic)

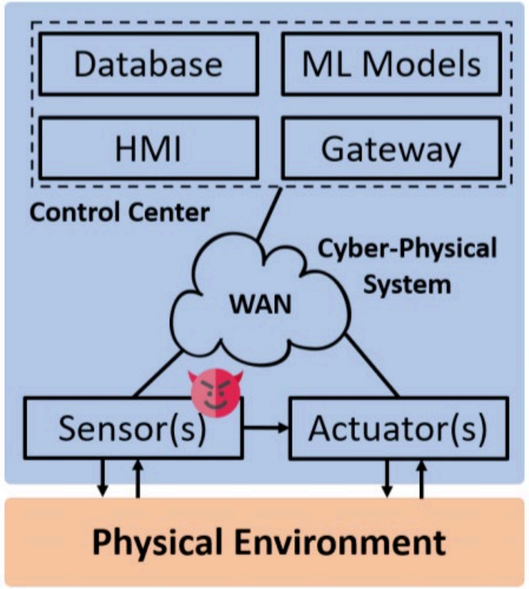
Secure Constrained Machine Learning for Critical Infrastructure CPS

Objective:

- Vulnerability assessment of machine learning models used for critical applications
- Design and development of secure machine learning models subject to physical and topological constraints using a defense-in-depth approach

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



Machine learning-assisted CPS

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

Achievement:

- The adversarial attacks successfully decreased the accuracy of the machine learning models to 0%-48.9% for different attacker capabilities