Security Certification of Autonomous Cyber-Physical Systems

Yier Jin[1] and Teng Zhang[2]

[1]University of Florida, [2]University of Central Florida

Email: yier.jin@ece.ufl.edu ; teng.zhang@ucf.edu

Challenges in Securing Autonomous CPS

- ❖Lack of knowledge of attacks (e.g. Denial of Service (DoS) and False data injection (FDI)) impact on the system level properties such as stability, safety, controllability, can lead the security solution developers to either over approximate or under approximate the damages that can be caused by an attack on the system;
- ❖ Attacks on sensors and network of CPS could be stealthy. Real-time solutions for detection and recovery of autonomous CPS from such attacks are lacking;
- ❖ Security solutions could be resource expensive and thus, impact the performance of the CPS.

Proposed Tasks

I. Study of relationship between attacks (DoS, FDI) and system level properties (e.g. safety, stability, controllability) of Autonomous CPS

- ❖ Incorporating noise and attacks in the Network Control System (NCS) model of autonomous CPS;
- ❖ To analyze the effect of attacks on stability, we transform the NCS model into hybrid system and use Lyapunov approach;
- ❖ To understand the impact of attacks on safety and controllability, we use an invariant computation approach.

II. Algorithms for detection and automatic recovery of CPS from attacks

- ❖ Design an optimal filter and a robust detector to simultaneously detect DoS or FDI attacks on sensors and estimate states of CPS;
- ❖ Design a resource efficient runtime monitor for detection of network attacks
- ❖ Evaluate robustness of detection mechanisms.

III. Quantifying impact of security solutions on design metrics of CPS

- ❖ Mapping a platform independent CPS model with security solution to a platform dependent model;
- ❖ Design contracts for performance, timing, computation and communication resources;
- ❖ Use quantitative model checking to verify that the platform dependent model with security solution satisfy the contracts.

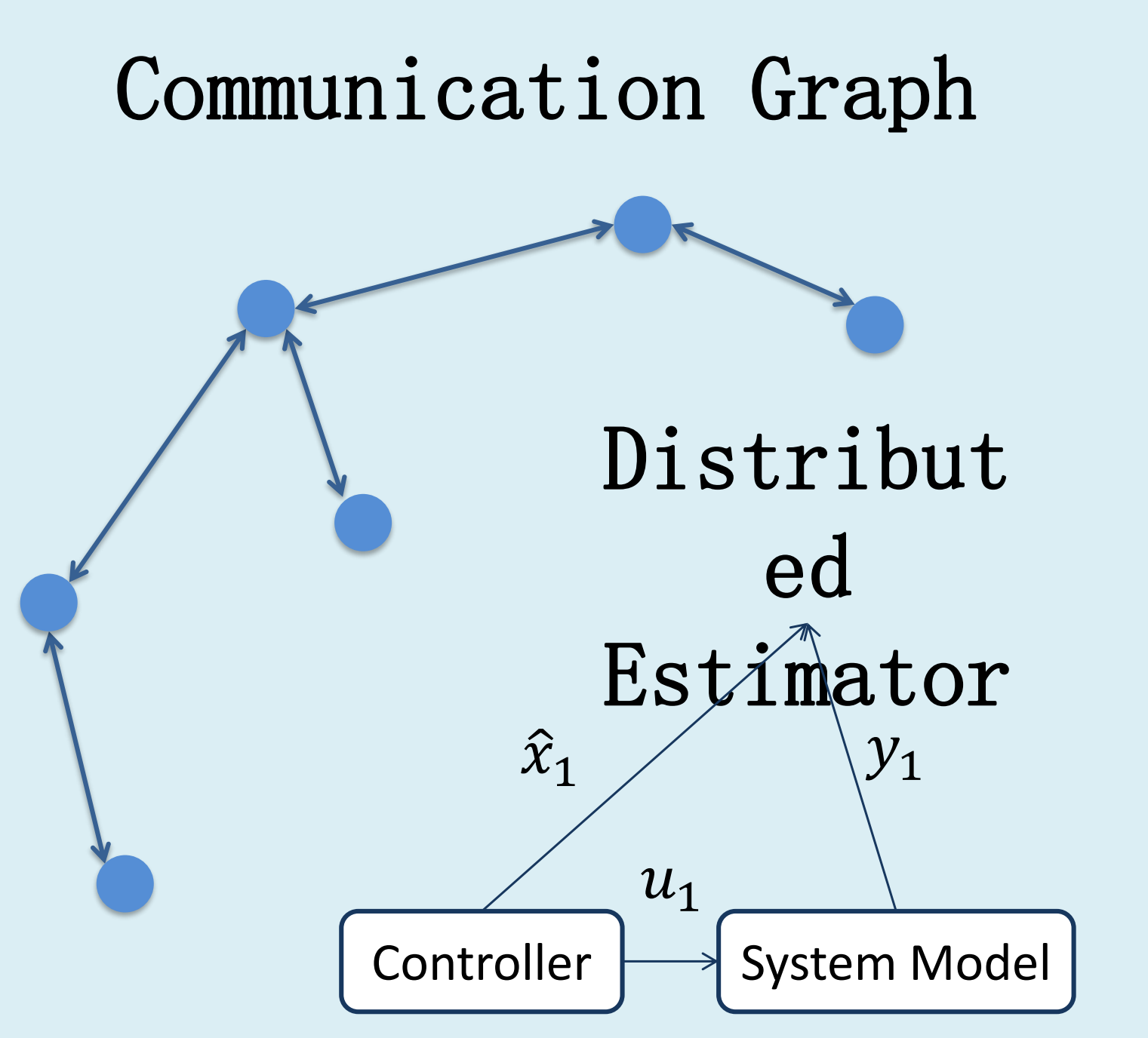
Fast Attack-Resilient Distributed State Estimator for Networked Cyber-Physical Systems

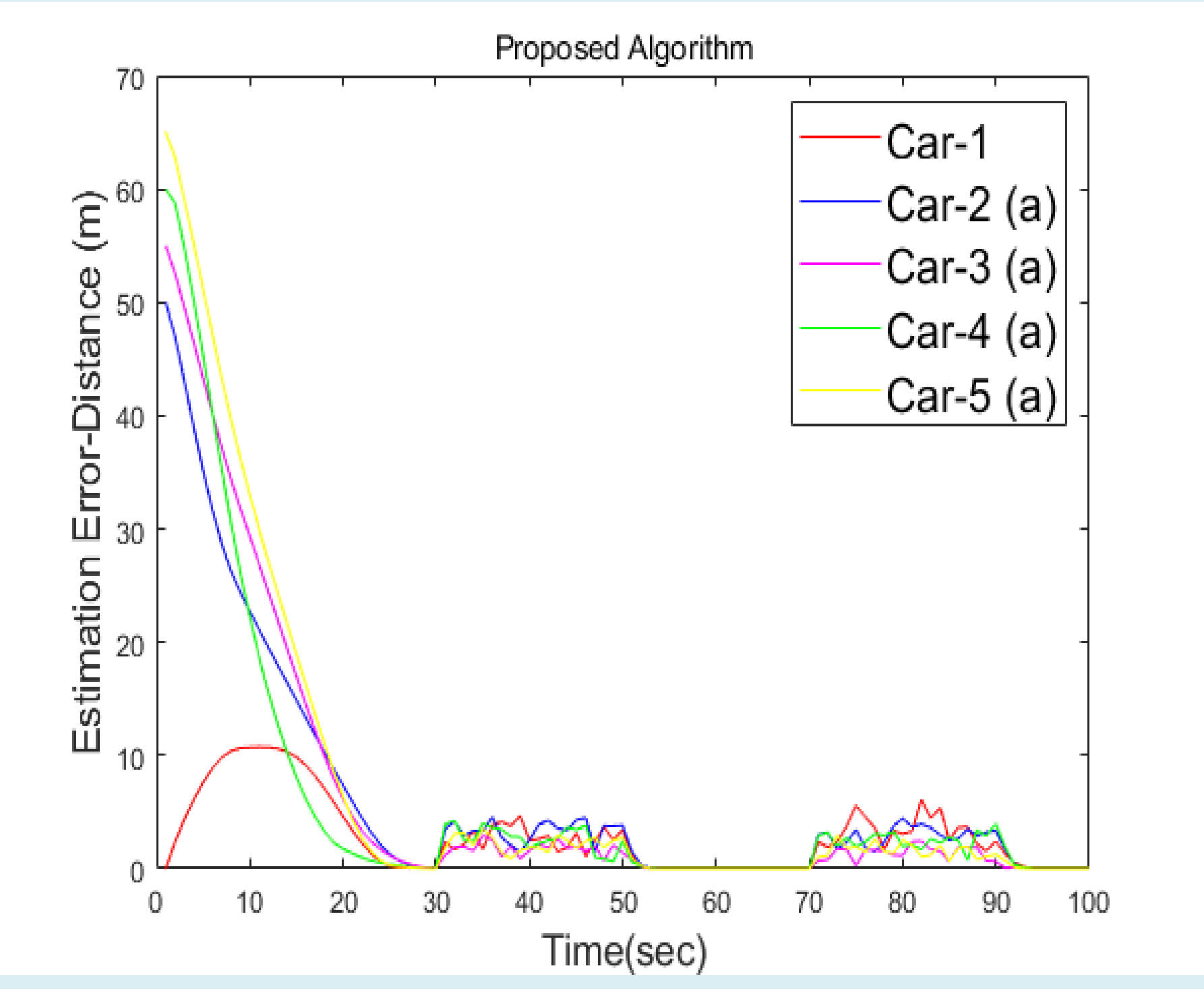
Goal: Develop a computationally efficient resilient distributed state estimator for networked CPS under sensor attack

Type of attack: False data injection on sensor measurements of multiple agents of the networked system

Goal of attack: Prevent agents from knowing the correct state of the system

Approach: Modify the Distributed Kalman Filter (DKF) by including an optimization step with close-form solutions that minimizes the total innovation of the DKF at each time





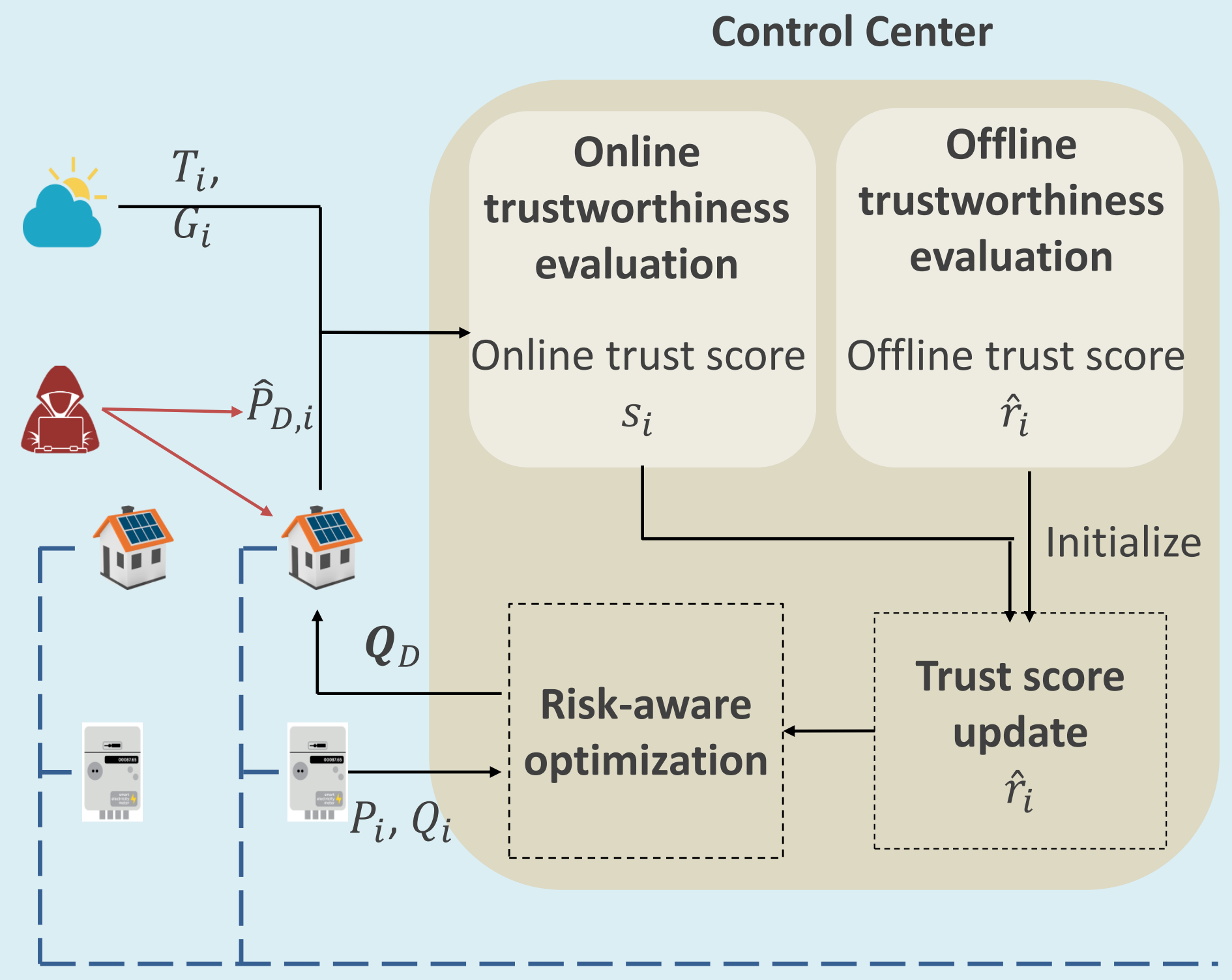
Risk-Aware Distributed Energy Resources (DER) Management Framework

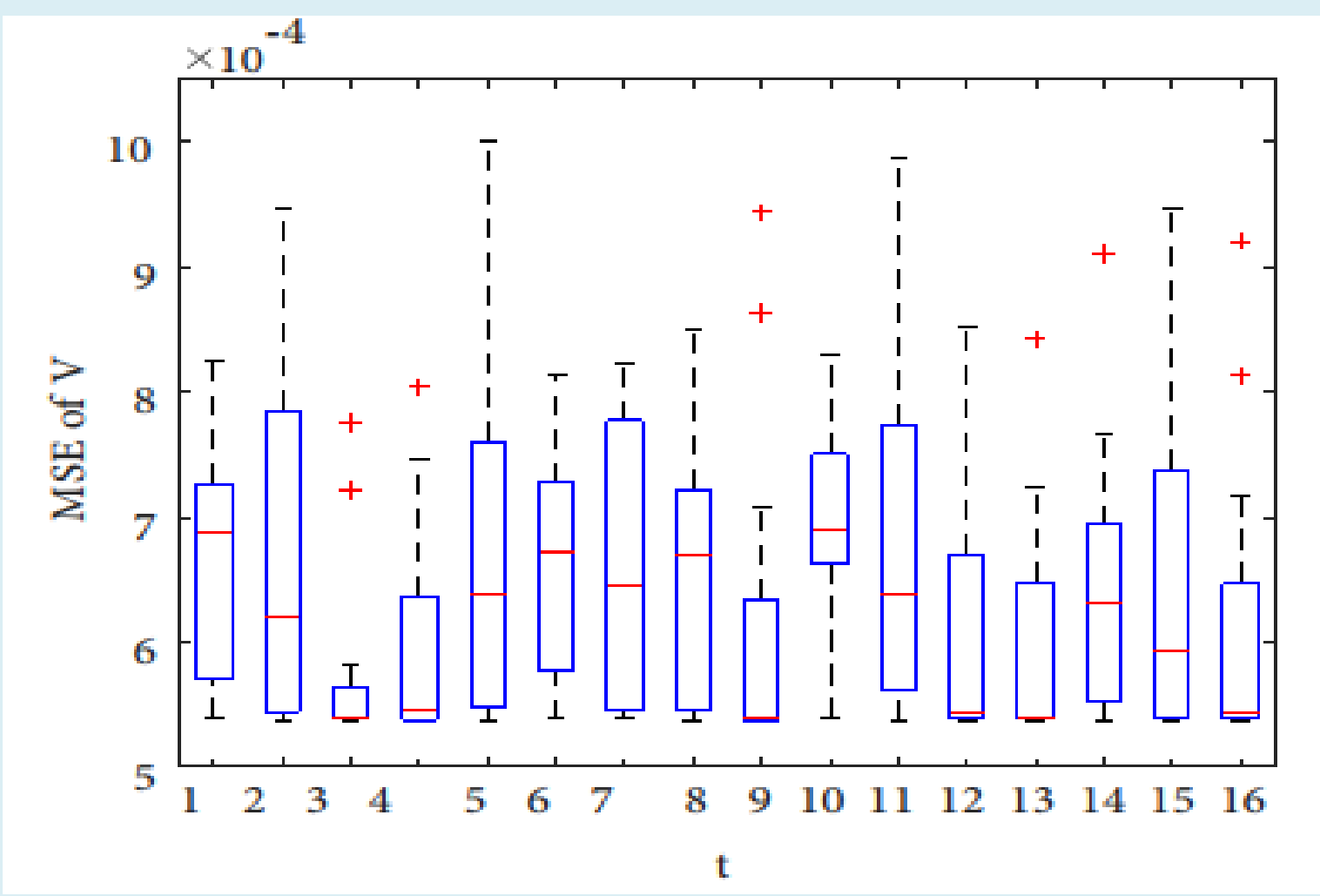
Goal: Develop a DER management framework for smart grid operators to coordination DERs under false data injection attacks

Type of attack: False data injection on sensor measurements of multiple DERs

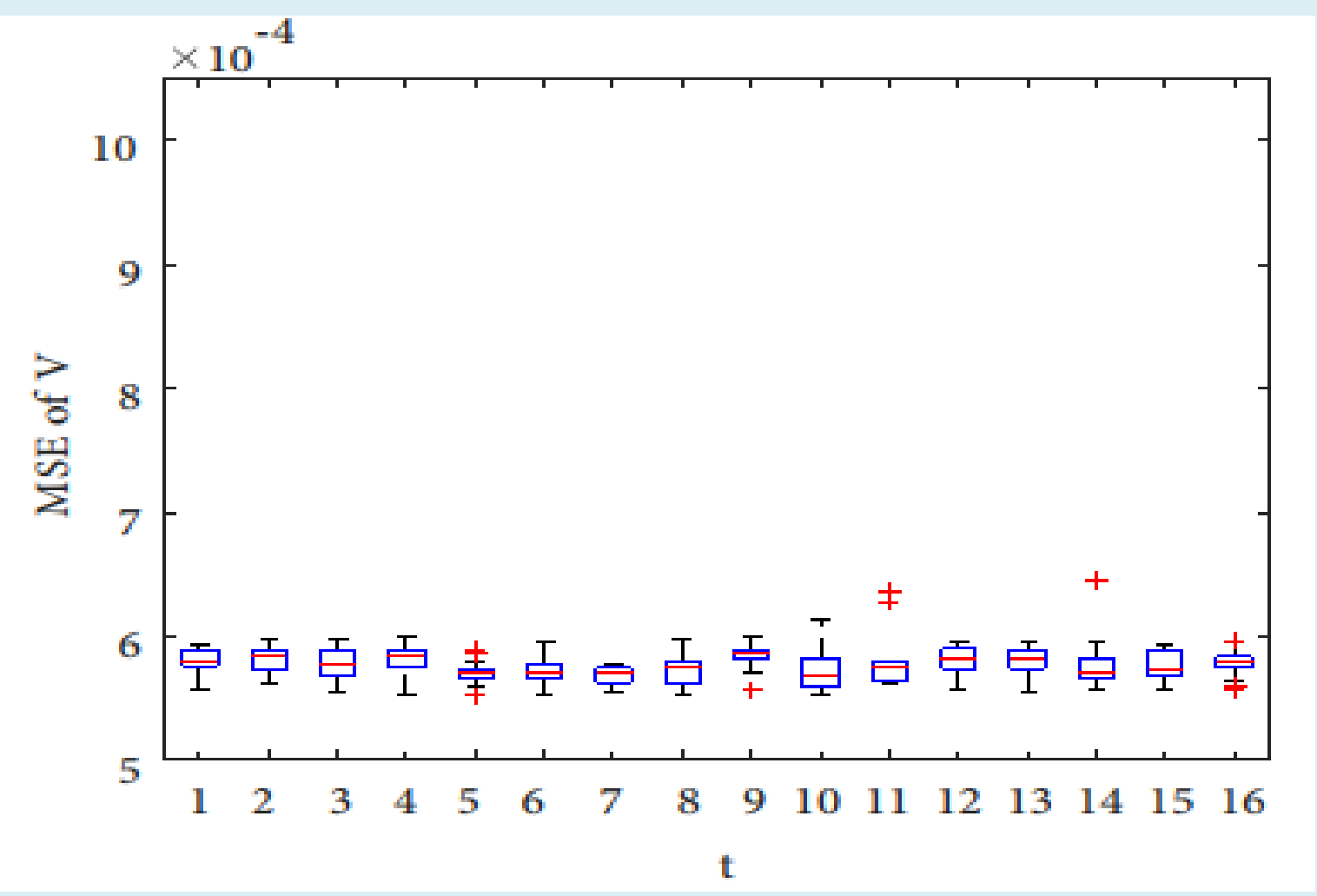
Goal of attack: Introduce errors to the control decisions for maintaining grid stability and economic operations

Approach: Combine the static and the real-time information to derive the probability that a DER is attacked, and utilize the probability to optimize the grid operations





No defense



Proposed scheme

Future Task: Securing Networked CPS

Task I: Design resilient DER coordination schemes with heterogeneous DERs.

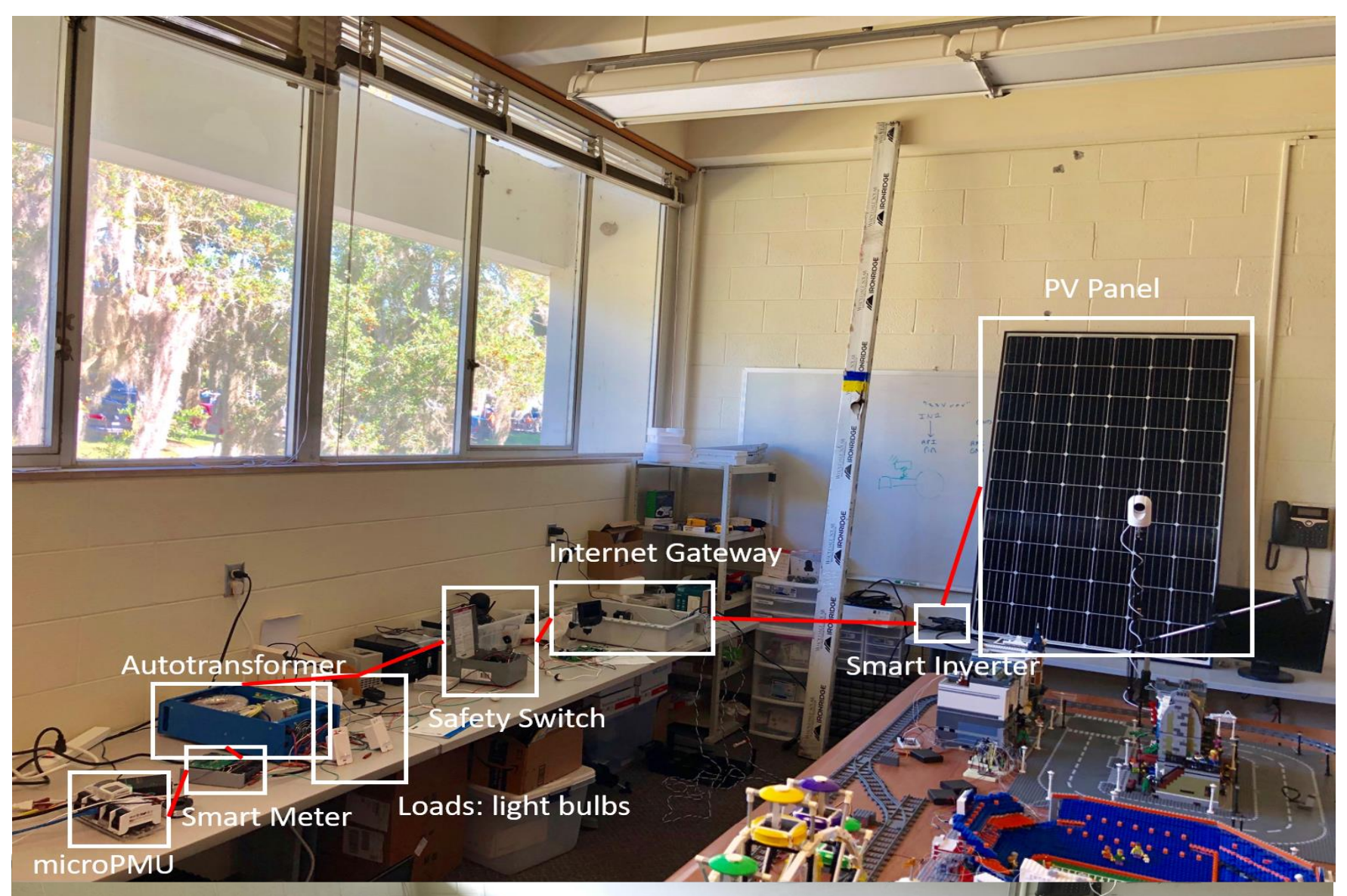
Task II: Specify security, communication resource, and timing as formal properties and verify them against the formal model of the system with the security method

Scientific Impacts

- ❖An in-depth study to understand the relationship between attacks and system level properties of autonomous CPS,
- ❖Design of novel real-time, detection and robust state estimation methods that can particularly aid mission critical CPS, which cannot be abruptly stopped after detection of an attack;
- ❖ Developing a novel framework that can support security solution developers in analyzing impact of their solution on design metrics of a resource constrained CPS

Broader Impacts and Educational Outreach

- ❖ Our proposed framework will have enormous impact, not only on our daily lives, but also on national security.
- ❖Engage high school students, undergraduates, and under-represented minorities in autonomous CPS and cybersecurity projects such as the smart grid and LEGO setup representing smart infrastructure.
- ❖Creating CPS security startup in Florida to support job growth and economic development of the region.



Project Outcomes

1.Feng Yu, RajGautam Dutta, Teng Zhang, Yaodan Hu and Yier Jin, “Fast Attack-Resilient Distributed State Estimator for Cyber-Physical Systems,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), 2020

2.Raj Gautam Dutta, Yaodan Hu, Feng Yu, Teng Zhang, and Yier Jin, “Design and Analysis of Secure Distributed Estimator for Vehicular Platooning in Adversarial Environment,” IEEE Transactions on Intelligent Transportation Systems (TITS), 2020

3.Yaodan Hu, Xiaochen Xian and Yier Jin, “RADM: A Risk-Aware DER Management Framework with Real-time DER Trustworthiness Evaluation,” 12th ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), 2021

4.Yaodan Hu, Haoqi Shan, Raj Gautam Dutta and Yier Jin, “P2SA: Protecting Platoons from Stealthy Jamming Attack,” Asian Hardware Oriented Security and Trust (AsianHOST), 2020

Principal Investigators’ Meeting

PI : Dr. Yier Jin ; **Co-PI:** Dr. Teng Zhang