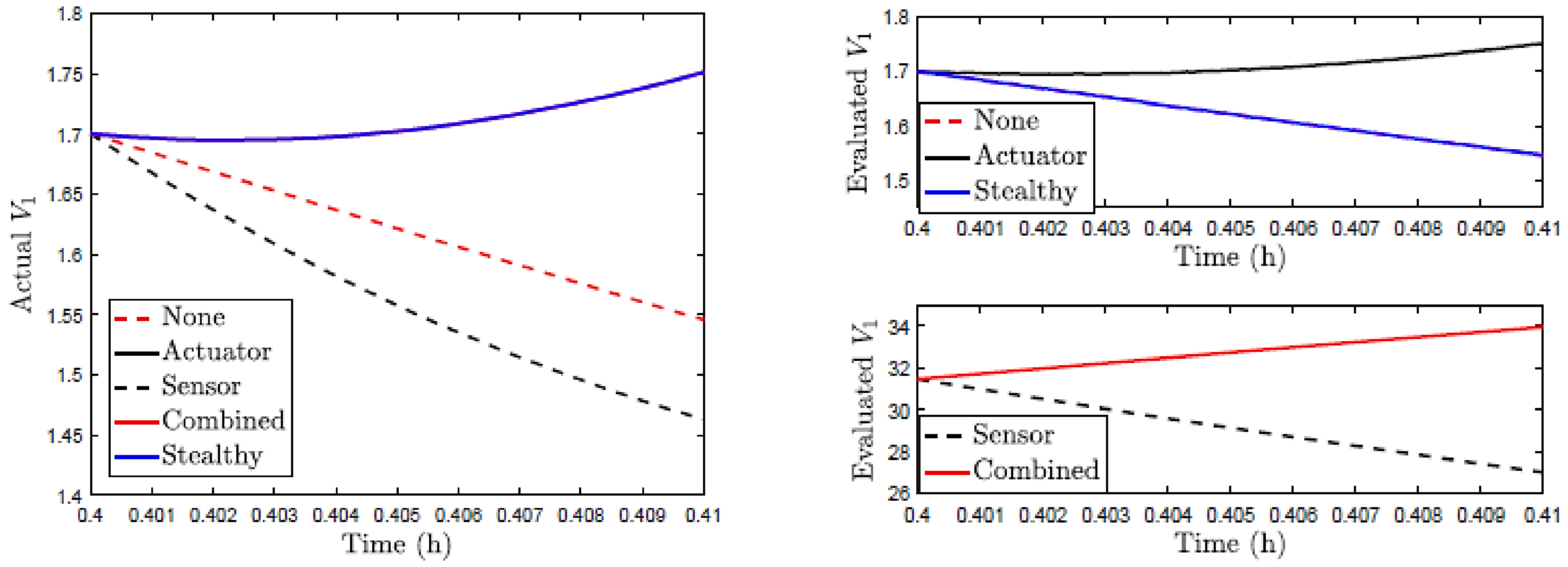
Enhancing Cybersecurity of Chemical Process Control Systems

Helen Durand, Wayne State University, Department of Chemical Engineering and Materials Science

Ph.D. Students Involved in the Work: Henrique Oyama, Kip Nieman, Keshav Kasturi Rangan, Dominic Messina

Cyberattacks on control systems can impact safety, production, and profits, and require constant vigilance and more restrictive technology adoption policies. We are developing control designs and theory for detecting attacks on nonlinear systems with the goal to create next-generation design policies for cyberattack-resilience.

- Cyberattacks are distinct from actuator and sensor faults
  - Deliberate efforts to conceal



Illustrative example:

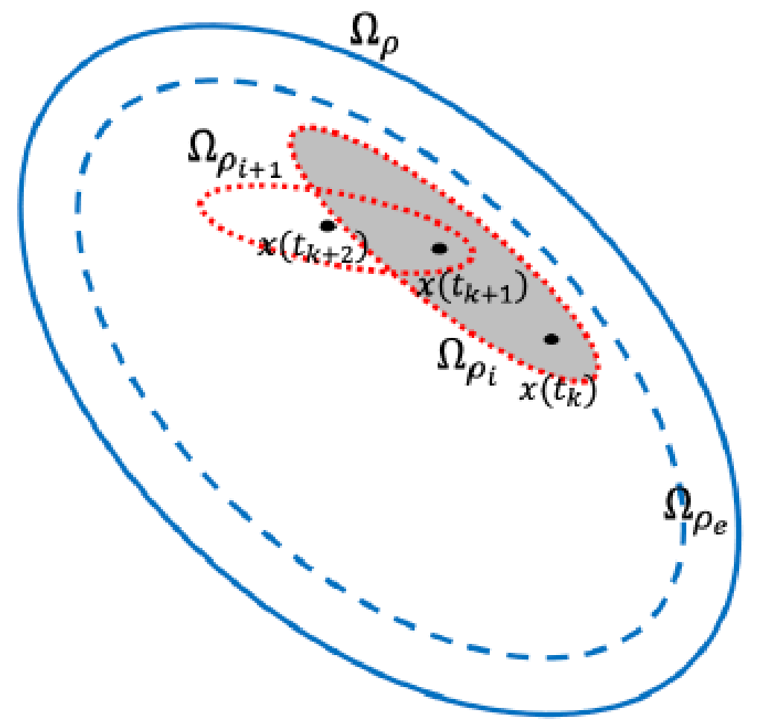
Bias attacks on actuator and sensor outputs vs. bias in actuator and "apparently correct" sensor trajectory

- Detecting cyberattacks using control-theoretic means adds to the toolbox of techniques available for enhanced security
  - Does it add enough value to warrant use?
    - Minimal security architecture
    - Next-generation system designs
  - Principles of design would extend across cyber-physical system domains
  - General control-theoretic developments for nonlinear systems

- Develop and evaluate techniques for handling attacks on actuators, sensors, and actuators and sensors at the same time (Oyama & Durand, *AIChE J.*, 2020; Rangan *et al.*, *DYCOPS*, 2022; Oyama *et al.*, *Frontiers in Chemical Engineering*, 2022)
  - Three detection policies: Passive (state estimation and state prediction-based) and active (Lyapunov function-based probing)
  - Modifications to strategies have different benefits for different attack types
  - Evaluate cyberattack-handling with image-based control and distributed control (Oyama *et al.*, *DYCOPS*, 2022; Oyama *et al.*, *Digital Chemical Engineering*, submitted)
- Consider attack detection policies making it difficult for an attacker to not be detected
  - Directed randomization

<u>Nested regions of control operation</u>:

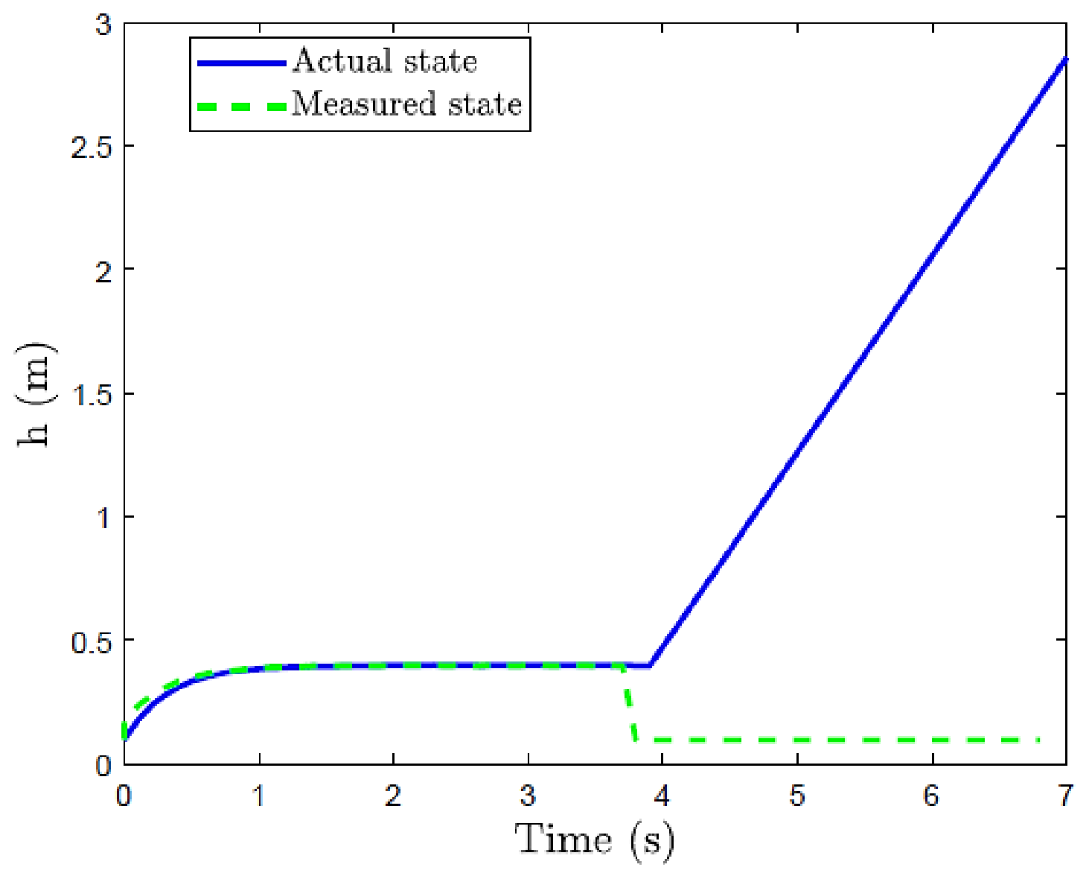
- <u>Active detection policy</u>: probe for cyberattacks by switching Lyapunov-based control formulations built upon a baseline safe region of operation (Ω_ρ)
- Control-theoretic guarantees related to the Lyapunov function profile for each region of operation



Broader Impacts

- Potential for reducing costs and risks to industry
- Students trained in REU experience
- Aided in aspects of training for 4 Ph.D. students
- Metro Detroit Youth Day and C2 Pipeline Summer Camps
- Animated short to YouTube

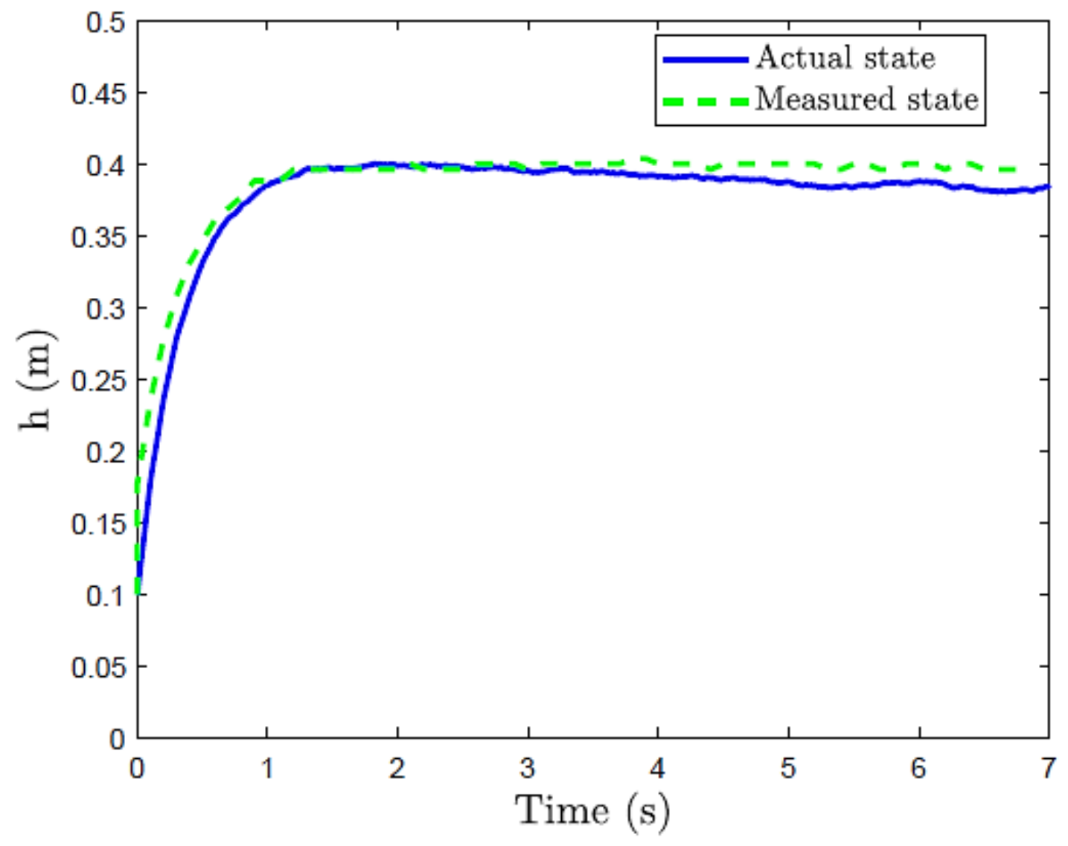
Example: Tank level measurements via camera images



(I)

Image replacement attacks:

Static (I) and stealthy (II) images



(II)

WAYNE STATE UNIVERSITY

Award ID#: 1932026