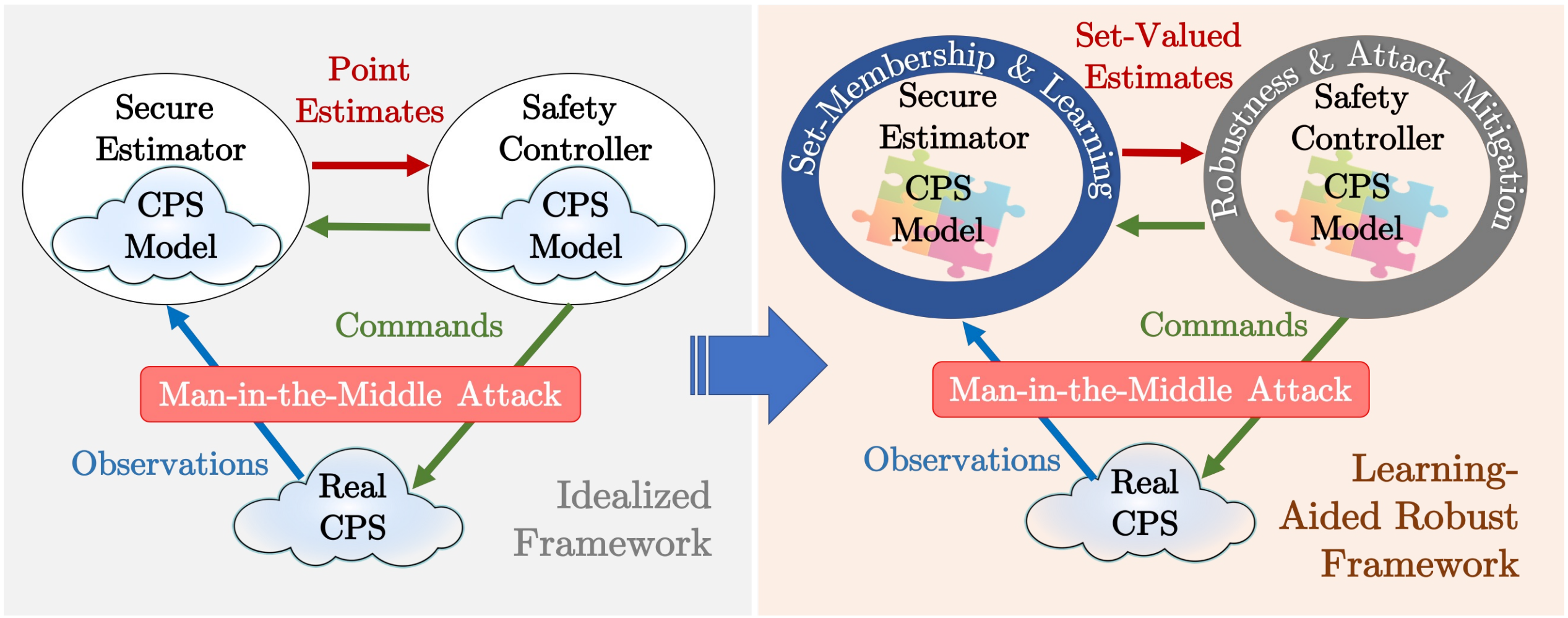
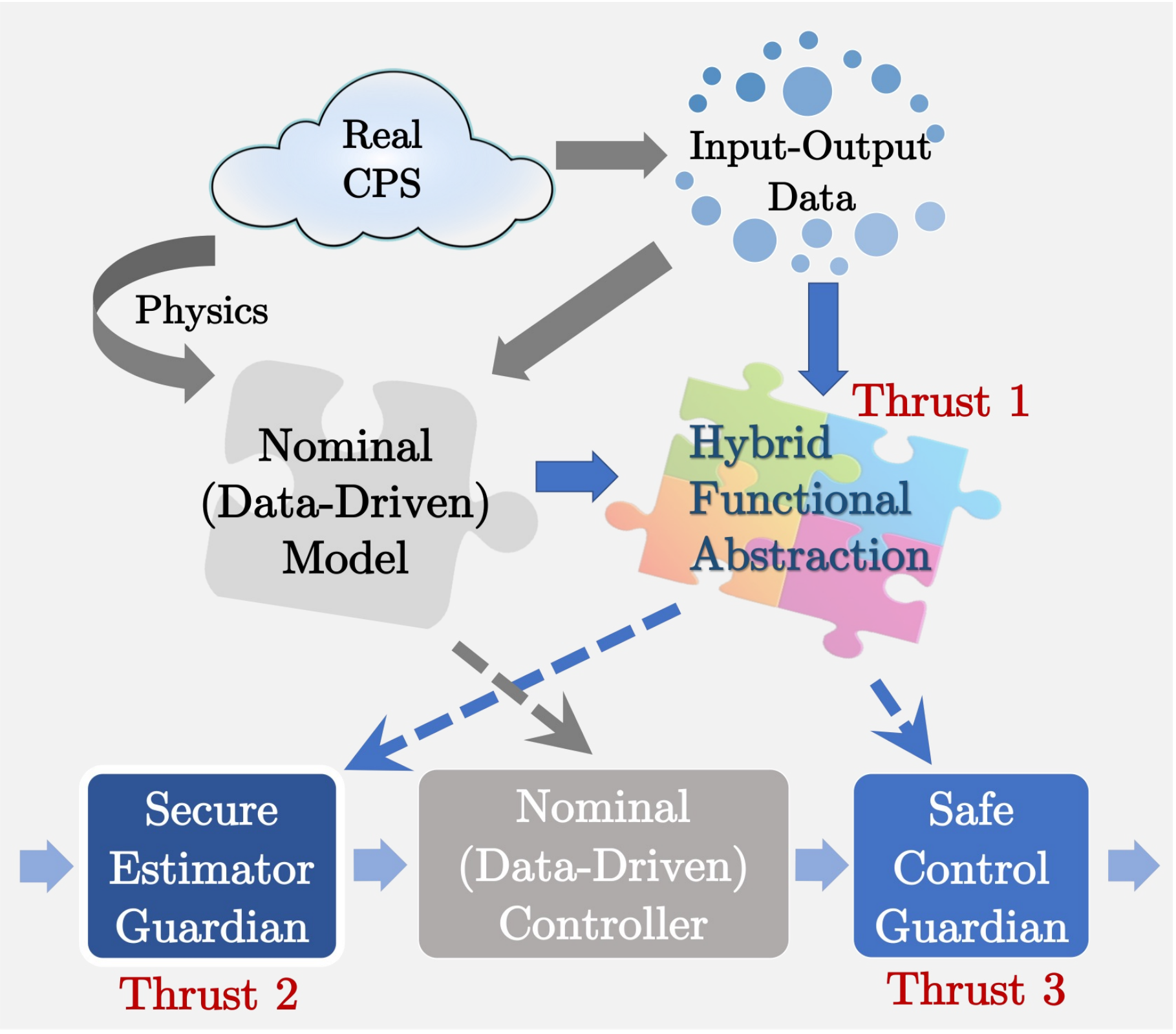
CAREER: Towards Non-Conservative Learning-Aided Robustness for Cyber-Physical Safety and Security

PI: Sze Zheng Yong, Mechanical and Industrial Engineering, Northeastern University (previously at Arizona State University)

Motivation




Real CPS
Input-Output Data
Physics
Nominal (Data-Driven) Model
Hybrid Functional Abstraction
Thrust 1
Secure Estimator Guardian
Thrust 2
Nominal (Data-Driven) Controller
Safe Control Guardian
Thrust 3

Problem and Objective

- Model mismatch between real system and imperfect model jeopardize safety and security guarantees
- How to quantify and learn uncertainty using set-inclusion models?
- How to design learning-aided secure state estimator despite man-in-the-middle attacks?
- How to non-conservatively "robustify" safety control algorithms?

Scientific Impacts

- Enable secure state estimators in the presence of set-valued uncertainties with run-time learning of attack models/strategies
- Develop safe-by-design control algorithms with attack-resilient output feedback designs with learning from run-time data
- Characterize various sources of uncertainties using inclusion models

Broader Impacts

Impact to Society

Application focus: : Self-driving cars

- Improving security and safety can save lives and ensure integrity of critical infrastructures

Broadly applicable methodology

- Can generalize to a broad class of CPS, e.g., power systems, medical devices

Education and Outreach

- Graduate student researchers: Syed Hassaan, Mohammad Khajenejad, Zeyuan Jin, Tarun Pati
- Broadening participation in computing and engineering plan targets undergraduate and graduate students at ASU/NU, especially first-generation students and includes engagement with industry.

Selected Publications

[1] Z. Jin, M. Khajenejad, M., and S.Z. Yong. "Robust Data-Driven Control Barrier Functions for Unknown Continuous Control Affine Systems." IEEE LCSS'23.

[2] T. Pati, S.Z. and Yong. "Robust Control Barrier Functions for Control Affine Systems with Time-Varying Parametric Uncertainties," IFAC-PapersOnLine'23.

[3] M. Khajenejad and S.Z. Yong. "Tight Remainder-Form Decomposition Functions with Applications to Constrained Reachability and Guaranteed State Estimation." IEEE TAC'23.

[4] T. Pati et al., "Interval Observers for Hybrid Dynamical Systems with Known Jump Times", IEEE CDC'23.

[5] M. Khajenejad et al. "Resilient State Estimation for Nonlinear Discrete-Time Systems via Input and State Interval Observer Synthesis", IEEE CDC'23.

Methods and Results

Robust Data-Driven Control Barrier Functions [1]:

$$\dot{x} = f(x) + g(x)u$$

- $h(x)$ is known
- $f(x)$ and $g(x)$ are unknown but continuous

$\Rightarrow$ $\dot{h}(x,u)$ is unknown but trajectory data is available

Approach: Set-Membership Learning:

$$\dot{h}(x,u) \geq -\alpha(h(x))$$

Lower bounds from data?

Assumption

The function $\dot{h} : \mathcal{X} \times \mathcal{U} \to \mathbb{R}$ is

- I globally Lipschitz continuous,
- II globally componentwise Lipschitz continuous, or
- III differentiable w.r.t. x and u with globally bounded Jacobians.

- I $\dot{h} \geq \dot{h}_i - L_x\|x - x_i\|_p - L_u\|u - u_i\|_p$
- II $\dot{h} \geq \dot{h}_i - L_x^\top|x - x_i| - L_u^\top|u - u_i|$
- III $\dot{h} \geq \dot{h}_i + \underline{J}_x\Delta x_i^+ - \overline{J}_x\Delta x_i^- + \underline{J}_u\Delta u_i^+ - \overline{J}_u\Delta u_i^-$ where $\Delta x_i \triangleq x - x_i$ and $\Delta u_i \triangleq u - u_i$.

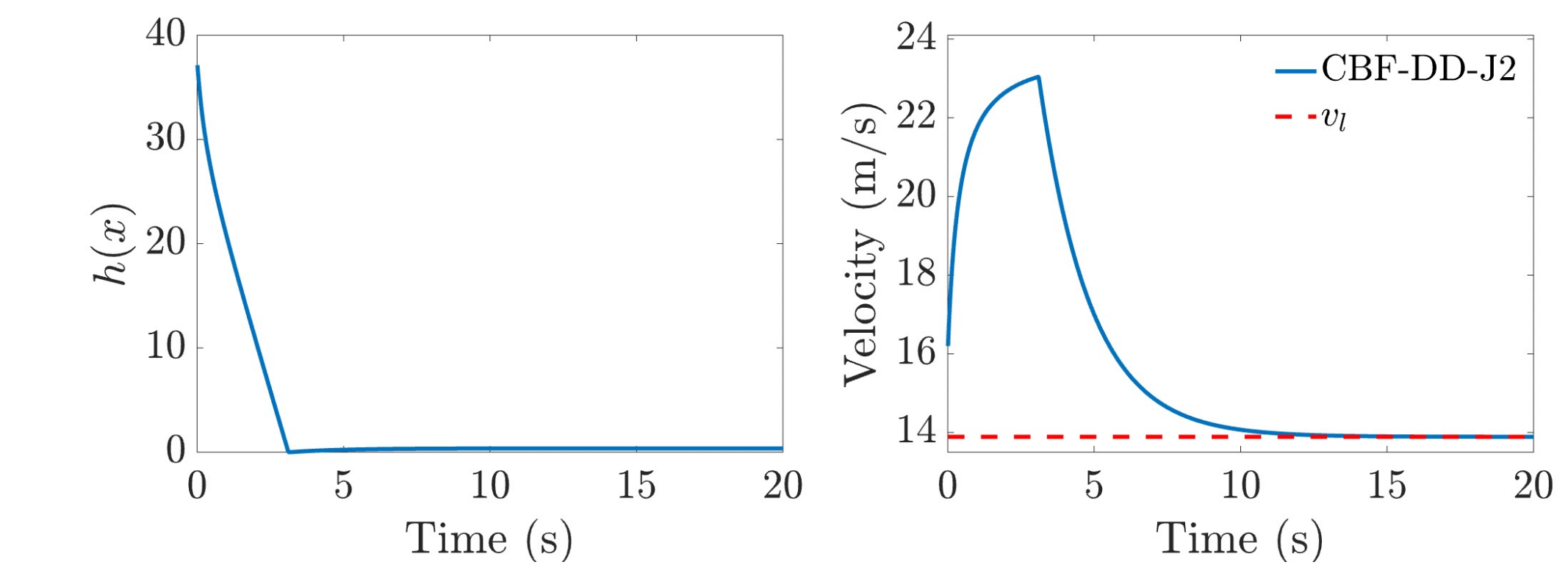


TABLE I: CPU time comparison for different methods.

Method	L	CL	J1	J2	SOCP [Taylor et al., 2021]
CPU time (s)	3029	3054	3154	2724	2.84×10^5

Robust CBFs with Parametric Uncertainties [2]:

$$\dot{x}(t) = f(x(t), \theta^*(t)) + g(x(t), \theta^*(t))u(t).$$

- State: $x(t) \in \mathcal{X} \subseteq \mathbb{R}^n$, Input: $u(t) \in \mathcal{U} \subset \mathbb{R}^m$
- Unknown parameter: $\theta^*(t) \in \Theta \subset \mathbb{R}^p$, and
- Unknown parameter variation: $\dot{\theta}^*(t) \in \Theta_d \subset \mathbb{R}^p$.

Method:

$$\dot{h}(x,u,\theta,\dot{\theta}) \geq -\alpha(h(x,\theta)), \qquad \forall \theta \in \Theta, \dot{\theta} \in \Theta_d$$

$$\textit{equivalently,} \quad \min_{\forall \theta, \dot{\theta}} \dot{h}(x,u,\theta,\dot{\theta}) + \alpha(h(x,\theta)) \geq 0,$$

Mixed-Monotone Decomposition Functions:

- *if* $\underline{\theta} \leq \theta \leq \overline{\theta} \quad \Rightarrow \quad f_d(\underline{\theta}, \overline{\theta}) \leq f(x,\theta) \leq f_d(\overline{\theta}, \underline{\theta})$

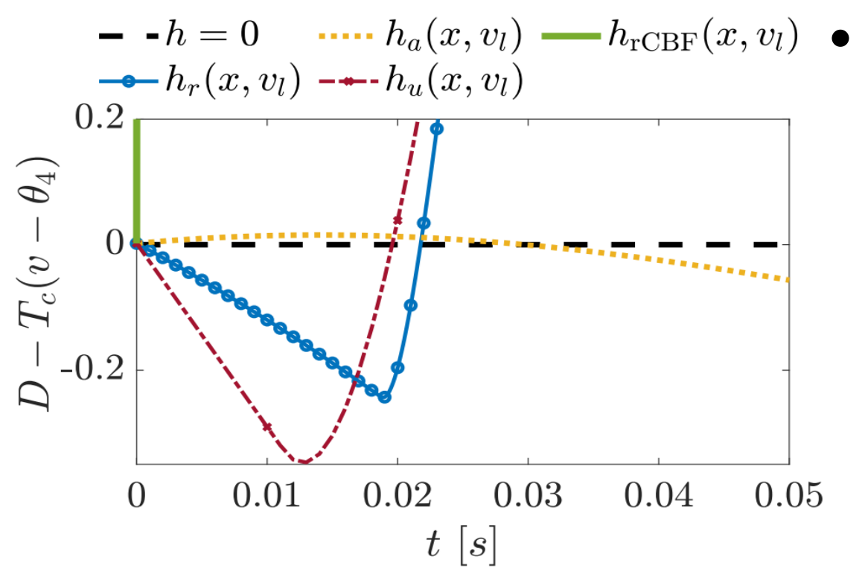
Concave Bounding:

- $\dot{h}(x,u,\theta,\dot{\theta}) \geq -\alpha(h(x,\theta)), \quad \forall \theta \in Ver(\Theta), \dot{\theta} \in Ver(\Theta_d)$

Dual LP: $\dot{h}(x,u,\theta,\dot{\theta}) + \alpha(h(x,\theta)) =$

$$(\phi(x) + \rho(x)u)^\top\theta + \psi(x)^\top\dot{\theta} + \sigma(x) + \tau(x)u$$

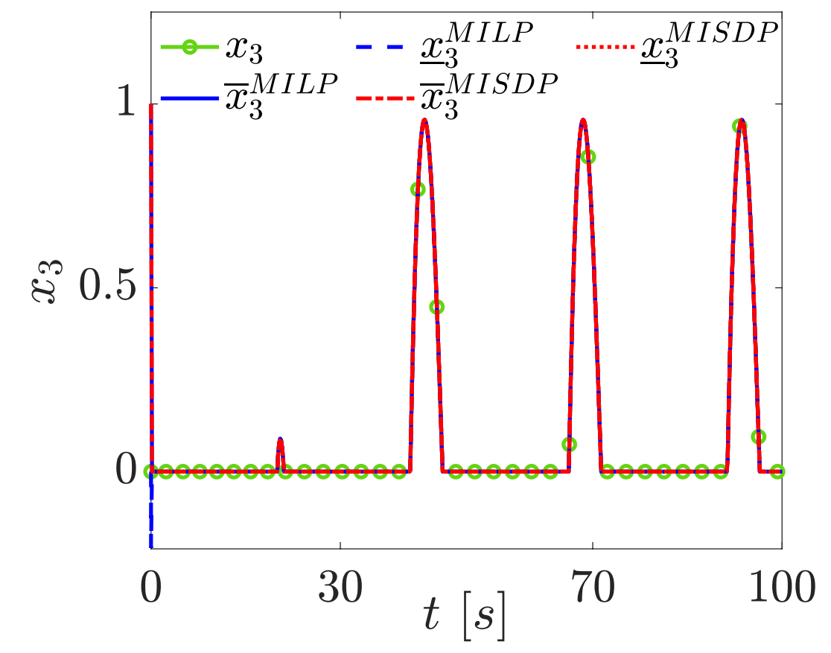
- *Dual:* $\inf_{\theta,\dot{\theta}} \ (\phi(x) + \rho(x)u)^\top\theta + \psi(x)^\top\dot{\theta} + \sigma(x) + \tau(x)u$
  s.t. $P_\theta\theta \leq q_\theta, P_{\theta_d}\dot{\theta} \leq q_{\theta_d}$



- Uncertainty-dependent CBFs (e.g., time-to-collision constraint) are satisfied, while adaptive/robust approaches does not.

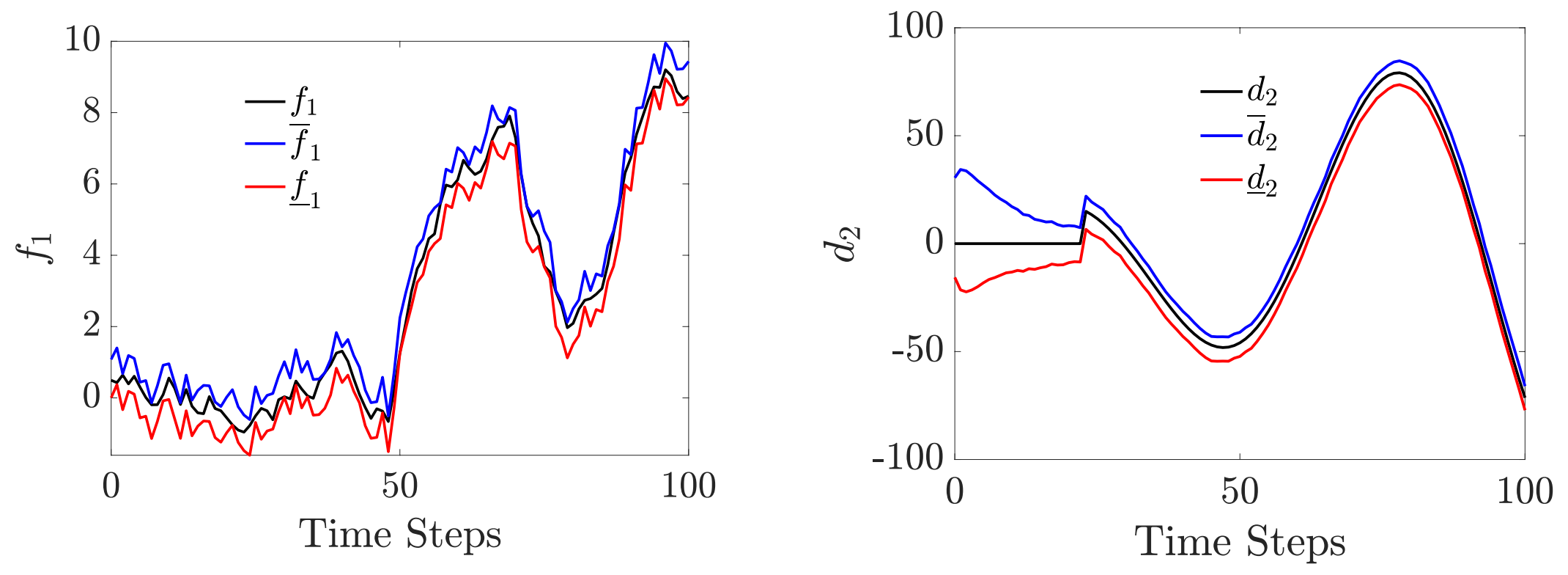
Tight Mixed-Monotone Decomposition Functions [3] and Interval Observers [4]:

- Designed a remainder-form mixed-monotone decomposition with the following properties:
  - Applicable to non-smooth, semi-continuous functions
  - Tightest in the family (that includes Yang et al. 2019)
  - Tractable/Computable in closed form.
- Leveraged mixed-monotone embedding systems for interval observer designs for continuous- and discrete-time and hybrid systems with known jumps.



Resilient State Estimation [5]:

- Designed interval observer for estimation of states and unknown inputs (with no known bounds or statistics).
- Leveraged system structure to cancel out the effects of the unknown inputs and utilized mixed-monotone decompositions to design a correct and stable observer.



Award ID#: 2313814