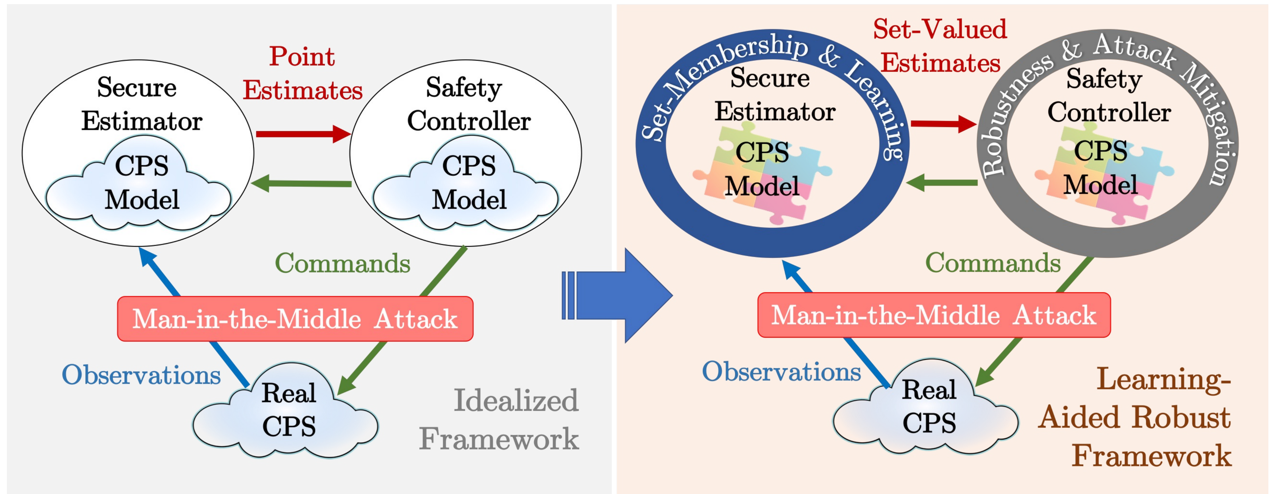
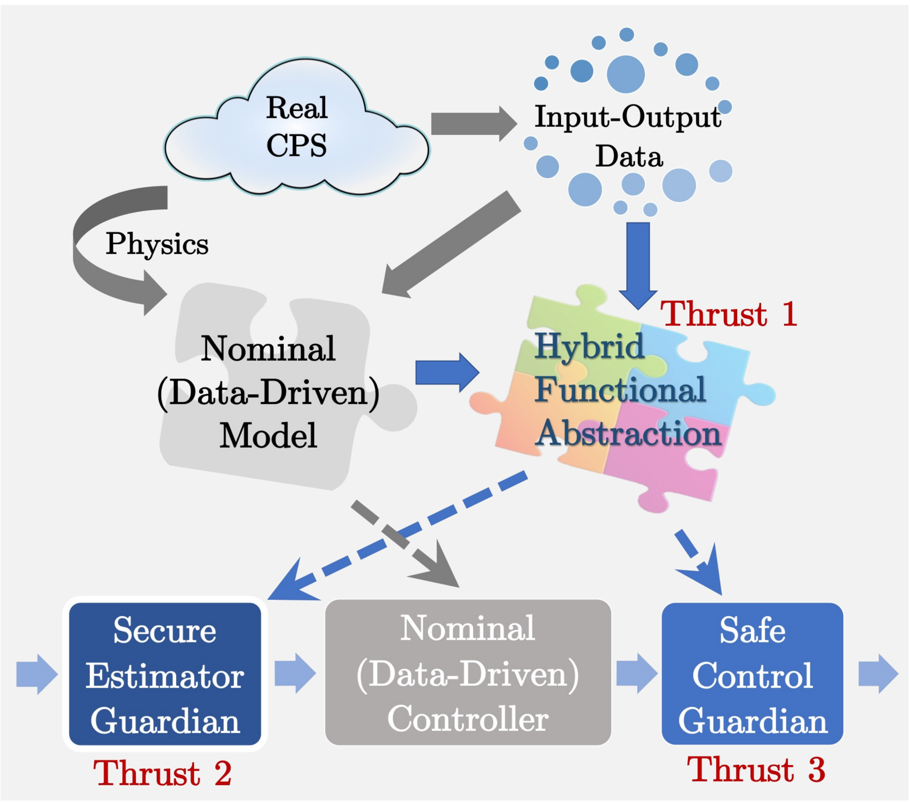
CAREER: Towards Non-Conservative Learning-Aided Robustness for Cyber-Physical Safety and Security

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

Motivation





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: Tarun Pati, Syed Hassaan, Mohammad Khajenejad, Zeyuan Jin, Maral Mordad
- 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] Pati, T. at al. "Limited Preview Control Barrier Functions for Continuous-Time Nonlinear Systems with Input Delays," IEEE CDC'24.

[2] Pati, T. et al. "Control Barrier Functions for Linear Continuous-Time Input-Delay Systems with Limited-Horizon Previewable Disturbances," ACC'2024.

[3] Hwang, S. et al. "Preventing Ankle Sprain: Integrating Preview Control Barrier Functions with Human Movement Primitive Prediction," IFAC CPHS'24.

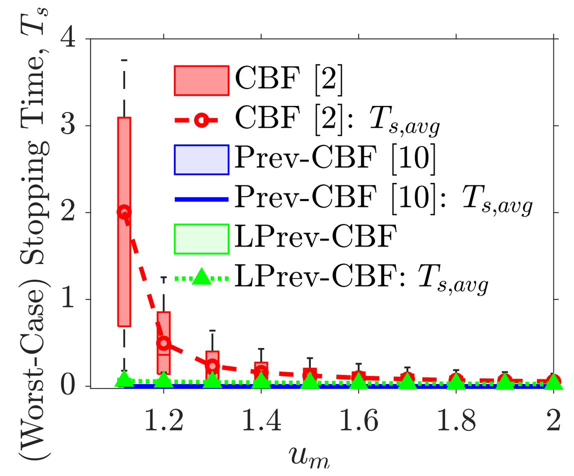
[4] Pati T. et al., "Computationally Efficient L1 and H_∞ Optimal Interval Observer Design", ECC'25, under review.

[5] Pati T. et al. "Polytopic Observer Designs for Uncertain Linear Systems", ECC'25, under review.

Methods and Results

Preview Control Barrier Functions with Algorithmic Linearization and Learning Methods [1–3]:

- Design robust controlled invariant safety controllers via CBFs that incorporate (limited-horizon) preview information, e.g., road curvature
  - Stopping time is decreased and intervention is less necessary

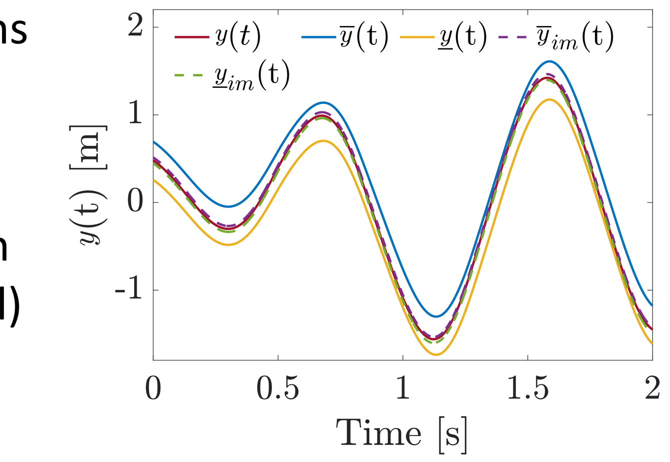


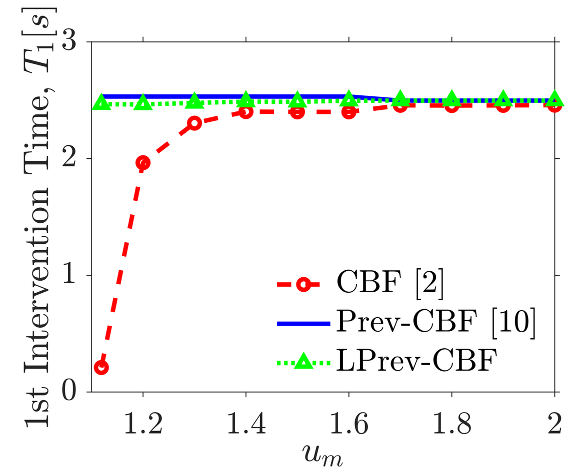
- Extended Prev-CBF to nonlinear systems via algorithmic linearization using Linear Programs
  - Method 1: Approximate linear model

$$f(z,d) = Az + Bu + B_d d + e_c + e_\ell$$

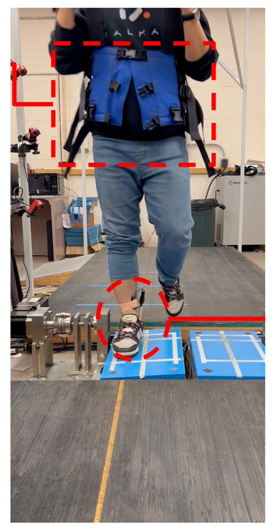
  - Method 2: Approximate linear immersion (higher-dimensional approx. linear model)

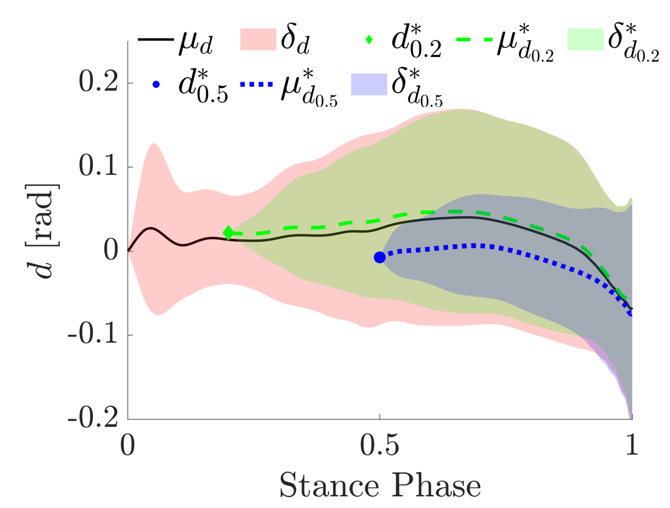
$$f^{(r)}(z,\mathbf{q}^r,u) = \sum_{l=0}^{r-1} \Gamma_l f^{(l)}(z,\mathbf{q}^{r-1}) + A_\ell z + B_{d,\ell}\mathbf{q}^r + B_{u,\ell}u + e_c + e_\ell$$

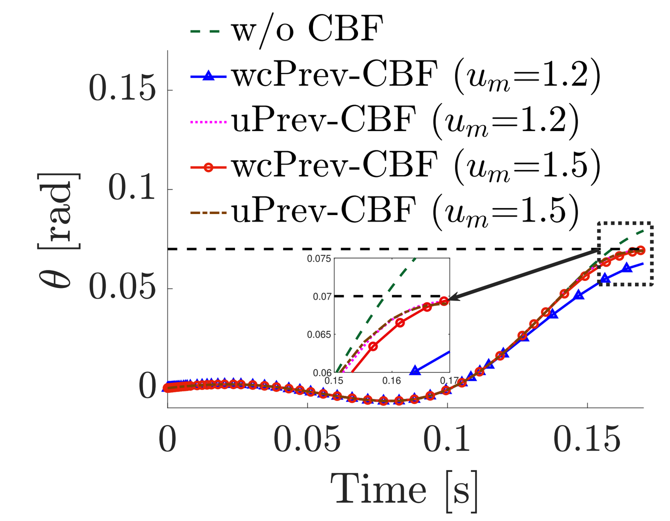


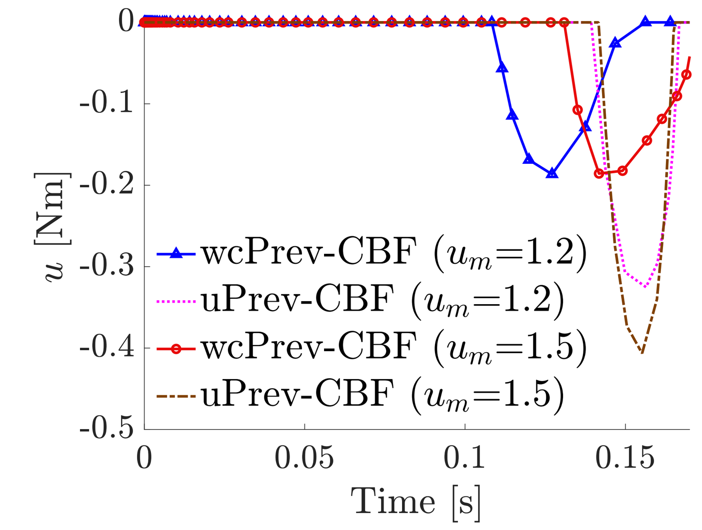


- Learned ankle motion model via Probabilistic Motion Primitives (ProMP) with uncertainty characterization and incorporated that uncertain model as preview information $\Longrightarrow$ reduced conservatism of Preview CBFs





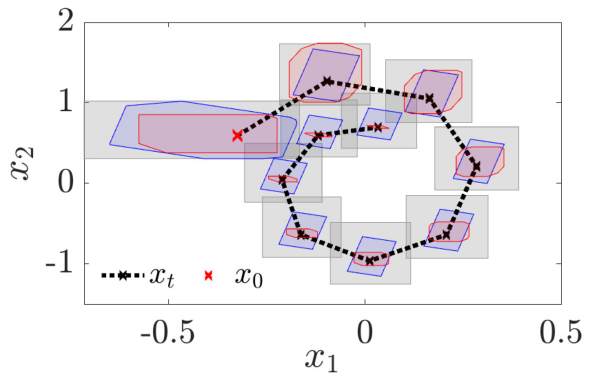


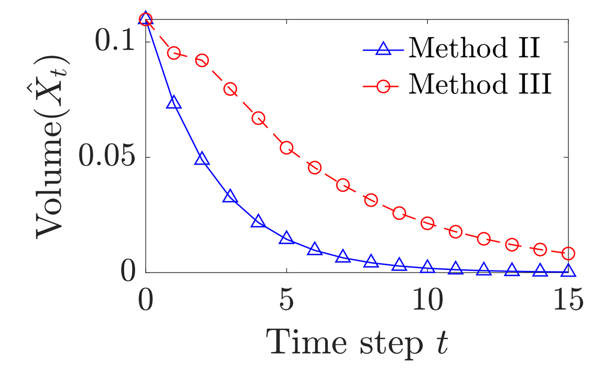


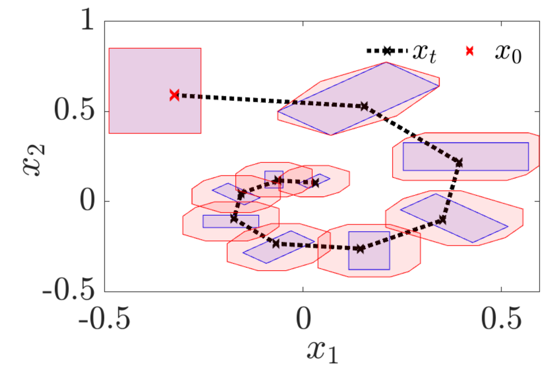
Interval [4] and Polytopic [5] Observers:

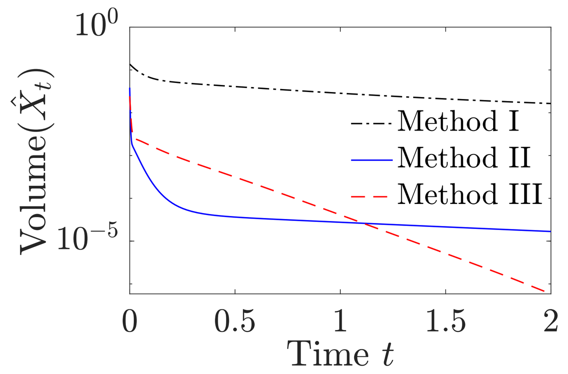
- Designed interval observers based mixed-monotone decomposition and reduced complexity of gain computation problem from MILP/MISDP to LP/SDP
- Designed one of the first polytopic observers for CT and DT systems $\Longrightarrow$ tighter than interval observers

Example		1	2	3	4	5	6	7	8
System Class		CT-L	CT-L	CT-L	CT-L	CT-L	DT-L	CT-N	DT-N
Sys. Dimension		2	3	12	12	6	2	3	2
$\mathcal{H}_\infty$	From [15]	0.29	0.34	0.97	1.01	0.45	0.48	0.32	0.77
	Proposed	0.25	0.25	0.27	0.32	0.25	0.40	0.22	0.58
L_1	From [15]	0.38	0.46	1.13	1.11	0.58	0.40	0.31	0.30
	Proposed	0.33	0.36	0.36	0.35	0.34	0.35	0.23	0.23









Award ID#: 2313814
(Previously, 1943545)