Remainder-Form Mixed-Monotone Decomposition Functions

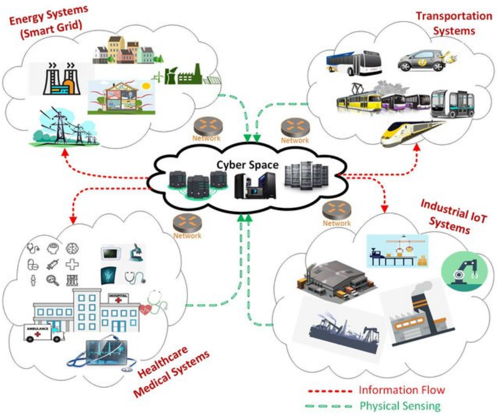
Mohammad Khajenejad

Department of Mechanical and Aerospace Engineering
University of California, San Diego, USA

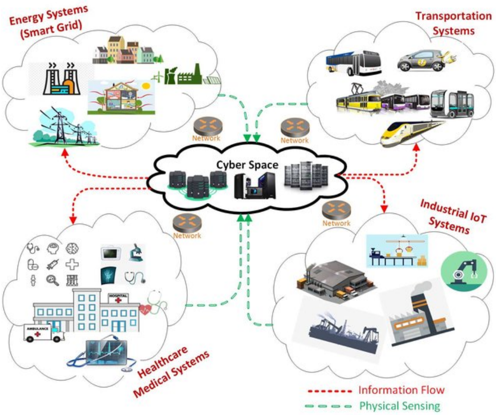
Email: mkhajenejad@ucsd.edu

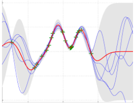
International Online Seminar on
Interval Methods in Control Engineering
May 25, 2023

Robust, Safe, Resilient, Private and Distributed Autonomy



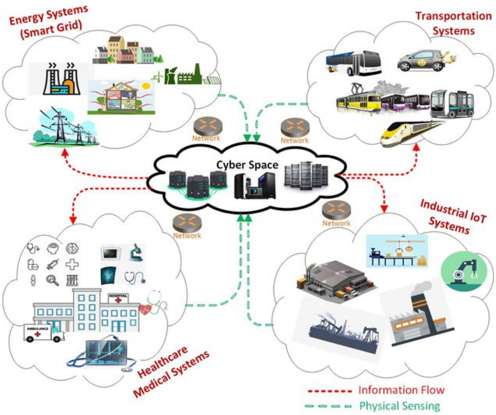
Robust, Safe, Resilient, Private and Distributed Autonomy

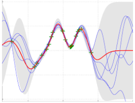




uncertainties $\Longrightarrow$ robustness

Robust, Safe, Resilient, Private and Distributed Autonomy

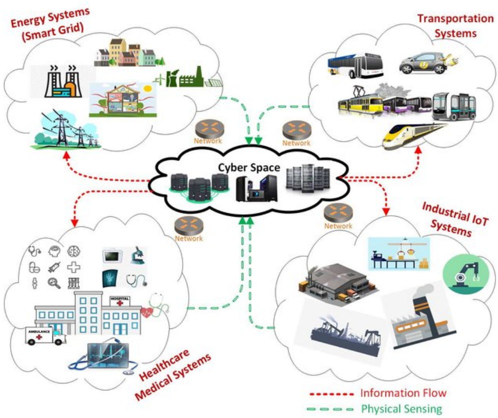


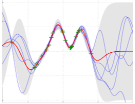


uncertainties $\Longrightarrow$ robustness

unsafe regions $\Longrightarrow$ safety critical

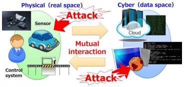
Robust, Safe, Resilient, Private and Distributed Autonomy





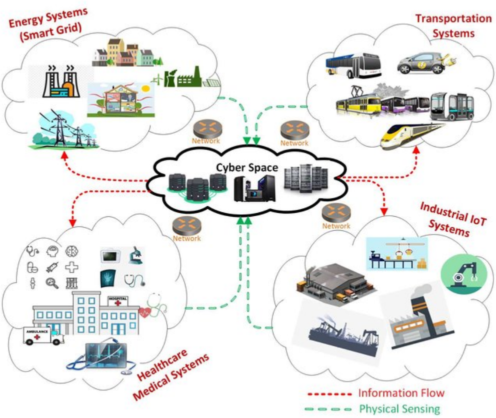
uncertainties $\Longrightarrow$ robustness

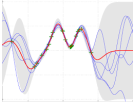
unsafe regions $\Longrightarrow$ safety critical



attacks $\Longrightarrow$ resiliency

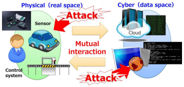
Robust, Safe, Resilient, Private and Distributed Autonomy



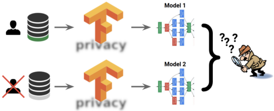


uncertainties $\Longrightarrow$ robustness

unsafe regions $\Longrightarrow$ safety critical

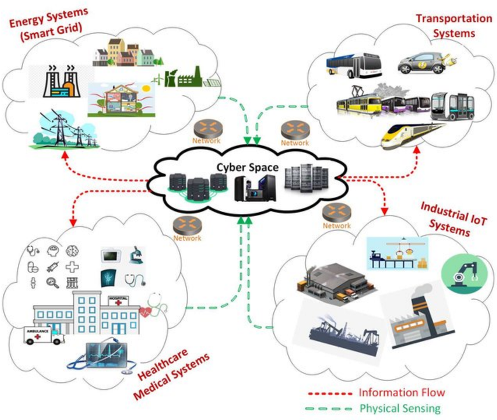


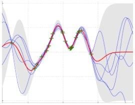
attacks $\Longrightarrow$ resiliency



data protection $\Longrightarrow$ privacy

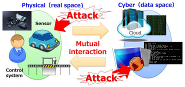
Robust, Safe, Resilient, Private and Distributed Autonomy



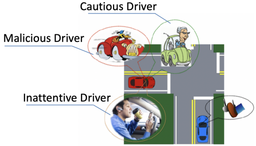


uncertainties $\Longrightarrow$ robustness

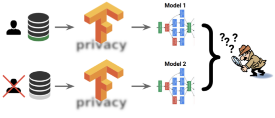
unsafe regions $\Longrightarrow$ safety critical



attacks $\Longrightarrow$ resiliency

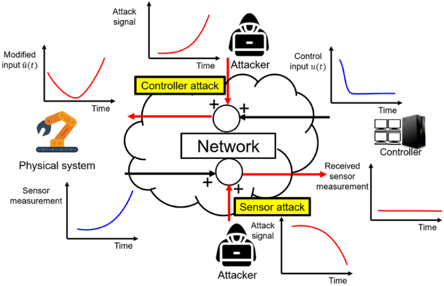


heterogeneous, local $\Longrightarrow$ networked cps



data protection $\Longrightarrow$ privacy

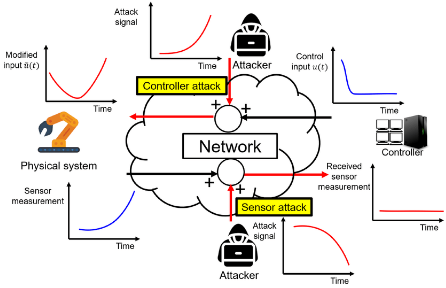
System Properties ⇒ Safe & Secure Autonomy



Research Question

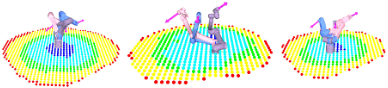
Can we leverage dynamic systems' properties to obtain robust, resilient, distributed & private autonomy?

System Properties ⇒ Safe & Secure Autonomy

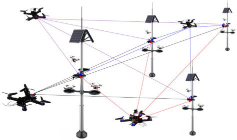


Research Question

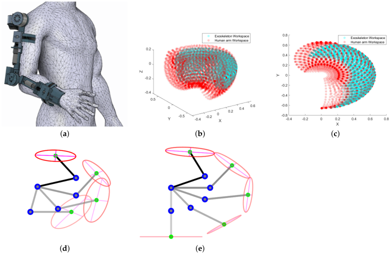
Can we leverage dynamic systems' properties to obtain robust, resilient, distributed & private autonomy?



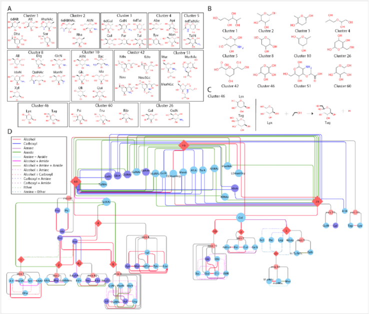
robot base placement



trajectories in swarm of drones



hybrid limb exoskeleton



Monosaccharide propagation

Outline; from Mixed-Monotonicity to...

- remainder-form decomposition functions

- applications:
  - set-valued state estimation
  - interval observer design
  - (distributed) resiliency

- future visions

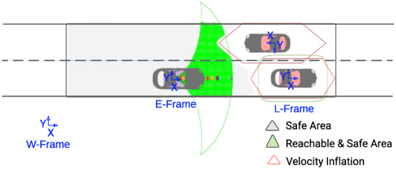
Outline; from Mixed-Monotonicity to...

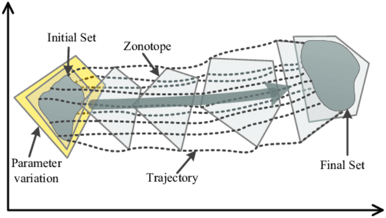
- remainder-form decomposition functions

- applications:
  - set-valued state estimation
  - interval observer design
  - (distributed) resiliency

- future visions

Set-Valued Robust Reachability Analysis

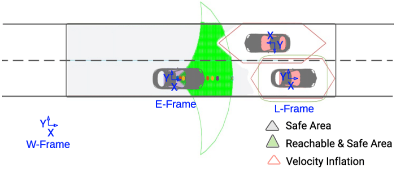


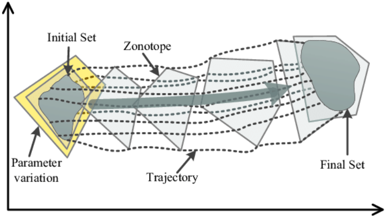


$$x^+ = f(\overbrace{x}^{\text{state}}, \underbrace{w}_{\text{bounded uncertainties}})$$

- Can be very challenging and computationally expensive for nonlinear systems

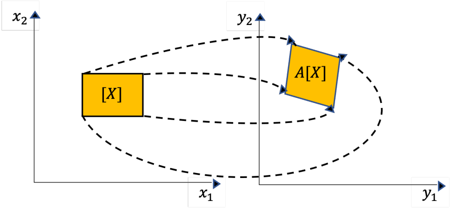
Set-Valued Robust Reachability Analysis





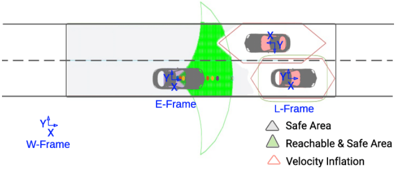
$$x^+ = f(\overbrace{x}^{\text{state}}, \underbrace{w}_{\text{bounded uncertainties}})$$

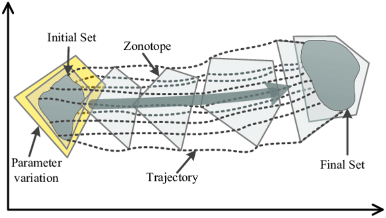
$x^+ = Ax$



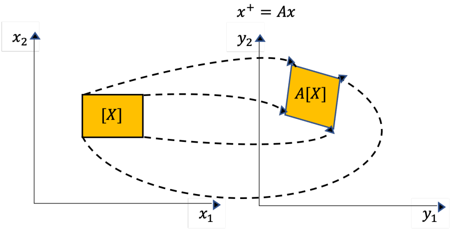
- Can be very challenging and computationally expensive for nonlinear systems

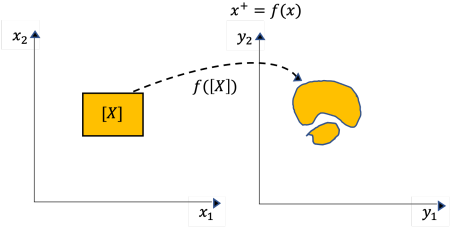
Set-Valued Robust Reachability Analysis





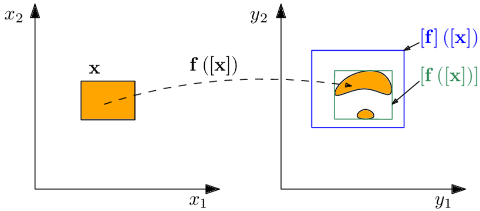
$$x^+ = f(\overbrace{x}^{\text{state}}, \underbrace{w}_{\text{bounded uncertainties}})$$





- Can be very challenging and computationally expensive for nonlinear systems

Reachability via Inclusion/Decomposition Functions



$$\underline{f} \leq \min_{x\in\mathcal{X}} f(x) \leq f(x) \leq \max_{x\in\mathcal{X}} f(x) \leq \overline{f} \Rightarrow [f](\mathcal{X}) = [\underline{f}, \overline{f}] \leftarrow \begin{cases} \text{natural inclusions} \\ \text{centered forms} \\ \text{mixed forms} \\ \text{Taylor forms} \\ \vdots \\ \text{mixed-monotone forms} \end{cases}$$

Problem 1

Given f and $\mathcal{X}$, can we find a tight and tractable inclusion function $[f]$?

Definition 2 (DT Decomposition Functions (Yang.ea.2019))

- $x_t^+ = f(x_t, w_t)$: a DT system, $f : \mathcal{Z} \to \mathbb{R}^n$
- $f_d : \mathcal{Z} \times \mathcal{Z} \to \mathbb{R}^n$: a DT-MMDF with respect to f, if
  - $f_d(z, z) = f(z)$
  - $\hat{z} \geq z \Rightarrow f_d(\hat{z}, z') \geq f_d(z, z')$
  - $\hat{z} \geq z \Rightarrow f_d(z', \hat{z}) \leq f_d(z', z)$

Definition 3 (CT Decomposition Functions (Abate.ea.2020))

- $x_t^+ = f(x_t, w_t)$: a CT system, $f : \mathcal{Z} \to \mathbb{R}^n$
- $f_d : \mathcal{Z} \times \mathcal{Z} \to \mathbb{R}^n$: a CT-MMDF with respect to f, if
  - $f_d(z, z) = f(z)$
  - $\hat{z} \geq z \wedge \hat{z}_i = z_i \Rightarrow f_{d,i}(\hat{z}, z') \geq f_{d,i}(z, z')$ (only "off-diagonal" arguments)
  - $\hat{z} \geq z \Rightarrow f_d(z', \hat{z}) \leq f_d(z', z)$

Mixed-Monotonicity & Decomposition Functions

Definition 2 (DT Decomposition Functions (Yang.ea.2019))

- $x_t^+ = f(x_t, w_t)$: a DT system, $f : \mathcal{Z} \to \mathbb{R}^n$
- $f_d : \mathcal{Z} \times \mathcal{Z} \to \mathbb{R}^n$: a DT-MMDF with respect to f, if
  - $f_d(z, z) = f(z)$
  - $\hat{z} \geq z \Rightarrow f_d(\hat{z}, z') \geq f_d(z, z')$
  - $\hat{z} \geq z \Rightarrow f_d(z', \hat{z}) \leq f_d(z', z)$

Definition 3 (CT Decomposition Functions (Abate.ea.2020))

- $x_t^+ = f(x_t, w_t)$: a CT system, $f : \mathcal{Z} \to \mathbb{R}^n$
- $f_d : \mathcal{Z} \times \mathcal{Z} \to \mathbb{R}^n$: a CT-MMDF with respect to f, if
  - $f_d(z, z) = f(z)$
  - $\hat{z} \geq z \wedge \hat{z}_i = z_i \Rightarrow f_{d,i}(\hat{z}, z') \geq f_{d,i}(z, z')$ (only "off-diagonal" arguments)
  - $\hat{z} \geq z \Rightarrow f_d(z', \hat{z}) \leq f_d(z', z)$

Embedding Systems

Definition 4 (Embedding Systems)

- $x_t^+ = f(x_t, w_t)$: an n-dimensional DT/CT system
- $x_0 \in [\underline{x}_0 \ \overline{x}_0]$, $w_t \in [\underline{w} \ \overline{w}]$
- $f_d(\cdot,\cdot)$: any decomposition function of f
- $2n$-dimensional embedding system:

$$\begin{bmatrix} \underline{x}_t^+ \\ \overline{x}_t^+ \end{bmatrix} = \begin{bmatrix} f_d([\underline{x}_t^\top \ \underline{w}^\top]^\top, [\overline{x}_t^\top \ \overline{w}^\top]^\top) \\ f_d([\overline{x}_t^\top \ \overline{w}^\top]^\top, [\underline{x}_t^\top \ \underline{w}^\top]^\top) \end{bmatrix} \tag{1}$$

Proposition 1

$$\underline{x}_t \leq x_t \leq \overline{x}_t, \forall t \geq 0, \forall w \in \mathcal{W}.$$

Definition 4 (Embedding Systems)

- $x_t^+ = f(x_t, w_t)$: an n-dimensional DT/CT system
- $x_0 \in [\underline{x}_0 \ \overline{x}_0]$, $w_t \in [\underline{w} \ \overline{w}]$
- $f_d(\cdot, \cdot)$: any decomposition function of f
- $2n$-dimensional embedding system:

$$\begin{bmatrix} \underline{x}_t^+ \\ \overline{x}_t^+ \end{bmatrix} = \begin{bmatrix} f_d([\underline{x}_t^\top \ \underline{w}^\top]^\top, [\overline{x}_t^\top \ \overline{w}^\top]^\top) \\ f_d([\overline{x}_t^\top \ \overline{w}^\top]^\top, [\underline{x}_t^\top \ \underline{w}^\top]^\top) \end{bmatrix} \tag{1}$$

Proposition 1

$$\underline{x}_t \leq x_t \leq \overline{x}_t, \forall t \geq 0, \forall w \in \mathcal{W}.$$

Existing Decomposition Functions

- "Optimal" (Abate.ea.2020):

$$f^{O}_{d,i}(z,\hat{z}) = \begin{cases} \min\limits_{\zeta\in[z,\hat{z}]} f_i(\zeta) & \text{if } z \le \hat{z}, \\ \max\limits_{\zeta\in[\hat{z},z]} f_i(\zeta) & \text{if } \hat{z} \le z. \end{cases}$$

- (Yang.ea.2019)

$$f^{L}_{d,i}(z,\hat{z}) = f_i(\zeta) + (\alpha_i - \beta_i)(z-\hat{z}),$$

$$\alpha_{ij} = \begin{cases} 0, & \text{Cases } 1,3,4,5, \\ |a_{ij}|, & \text{Case } 2, \end{cases}, \ \beta_{ij} = \begin{cases} 0, & \text{Cases } 1,2,4,5, \\ -|b_{ij}|, & \text{Case } 3, \end{cases},$$

$$\zeta_j = \begin{cases} z_j, & \text{Cases } 1,2,5, \\ \hat{z}_j, & \text{Cases } 3,4, \end{cases}$$

Case 1 : $a_{ij} \ge 0$, Case 2 : $a_{ij} \le 0, b_{ji} \ge 0, |a_{ij}| \le |b_{ij}|$, Case 3 : $a_{ij} \le 0, b_{ij} \ge 0, |a_{ij}| \ge |b_{ij}|$, Case 4 : $b_{ij} \le 0$, Case 5: $j = i$

Existing Decomposition Functions

- "Optimal" (Abate.ea.2020):

$$f^O_{d,i}(z,\hat{z}) = \begin{cases} \min_{\zeta \in [z,\hat{z}]} f_i(\zeta) & \text{if } z \leq \hat{z}, \\ \max_{\zeta \in [\hat{z},z]} f_i(\zeta) & \text{if } \hat{z} \leq z. \end{cases}$$

- (Yang.ea.2019)

$$f^L_{d,i}(z,\hat{z}) = f_i(\zeta) + (\alpha_i - \beta_i)(z - \hat{z}),$$

$$\alpha_{ij} = \begin{cases} 0, & \text{Cases } 1,3,4,5, \\ |a_{ij}|, & \text{Case } 2, \end{cases}, \quad \beta_{ij} = \begin{cases} 0, & \text{Cases } 1,2,4,5, \\ -|b_{ij}|, & \text{Case } 3, \end{cases},$$

$$\zeta_j = \begin{cases} z_j, & \text{Cases } 1,2,5, \\ \hat{z}_j, & \text{Cases } 3,4, \end{cases}$$

Case 1 : $a_{ij} \geq 0$, Case 2 : $a_{ij} \leq 0, b_{ji} \geq 0, |a_{ij}| \leq |b_{ij}|$, Case 3 : $a_{ij} \leq 0, b_{ij} \geq 0, |a_{ij}| \geq |b_{ij}|$, Case 4 : $b_{ij} \leq 0$, Case 5: $j = i$

Existing Decomposition Functions

- "Optimal" (Abate.ea.2020):

$$f^{O}_{d,i}(z,\hat{z}) = \begin{cases} \min\limits_{\zeta\in[z,\hat{z}]} f_i(\zeta) & \text{if } z \leq \hat{z}, \\ \max\limits_{\zeta\in[\hat{z},z]} f_i(\zeta) & \text{if } \hat{z} \leq z. \end{cases}$$

- (Yang.ea.2019)

$$f^{L}_{d,i}(z,\hat{z}) = f_i(\zeta) + (\alpha_i - \beta_i)(z - \hat{z}),$$

$$\alpha_{ij} = \begin{cases} 0, & \text{Cases } 1,3,4,5, \\ |a_{ij}|, & \text{Case } 2, \end{cases}, \ \beta_{ij} = \begin{cases} 0, & \text{Cases } 1,2,4,5, \\ -|b_{ij}|, & \text{Case } 3, \end{cases},$$

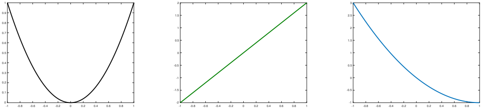
$$\zeta_j = \begin{cases} z_j, & \text{Cases } 1,2,5, \\ \hat{z}_j, & \text{Cases } 3,4, \end{cases}$$

Case 1 : $a_{ij} \geq 0$, Case 2 : $a_{ij} \leq 0, b_{ji} \geq 0, |a_{ij}| \leq |b_{ij}|$, Case 3 : $a_{ij} \leq 0, b_{ij} \geq 0, |a_{ij}| \geq |b_{ij}|$, Case 4 : $b_{ij} \leq 0$, Case 5: $j = i$

Remainder-Form Mixed-Monotone Decompositions

Khajenejad, M. and Yong, S.Z. "Tight Remainder-Form Decomposition Functions with Applications to Constrained Reachability and Guaranteed State Estimation." *IEEE Transactions on Automatic Control*, 2023, accepted, (Impact Factor = 6.549).

$$f(x) = \underbrace{Hx}_{\text{linear remainder}} + \underbrace{g(x)}_{\text{JSS mapping}}, H_{i,j} = \overline{J}^f_{i,j} \vee H_{i,j} = \underline{J}^f_{i,j}$$



$$H^{\oplus}\underline{x} - H^{\ominus}\overline{x} \leq Hx \leq H^{\oplus}\overline{x} - H^{\ominus}\underline{x}$$

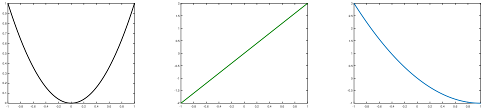
$$g(\underline{x}_c) \leq g(x) \leq g(\overline{x}_c)$$

$$\underbrace{H^{\oplus}\underline{x} - H^{\ominus}\overline{x} + g(\underline{x}_c)}_{f_d(\underline{x},\overline{x})} \leq \underbrace{Hx + g(x)}_{f(x)} \leq \underbrace{H^{\oplus}\overline{x} - H^{\ominus}\underline{x} + g(\overline{x}_c)}_{f_d(\overline{x},\underline{x})}$$

Remainder-Form Mixed-Monotone Decompositions

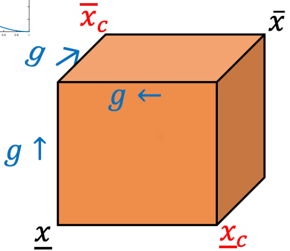
Khajenejad, M. and Yong, S.Z. "Tight Remainder-Form Decomposition Functions with Applications to Constrained Reachability and Guaranteed State Estimation." *IEEE Transactions on Automatic Control*, 2023, accepted, (Impact Factor = 6.549).

$$f(x) = \underbrace{Hx}_{\text{linear remainder}} + \underbrace{g(x)}_{\text{JSS mapping}} \quad , H_{i,j} = \overline{J}^f_{i,j} \vee H_{i,j} = \underline{J}^f_{i,j}$$



$$H^{\oplus}\underline{x} - H^{\ominus}\overline{x} \leq Hx \leq H^{\oplus}\overline{x} - H^{\ominus}\underline{x}$$

$$g(\underline{x}_c) \leq g(x) \leq g(\overline{x}_c)$$

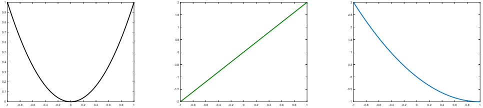


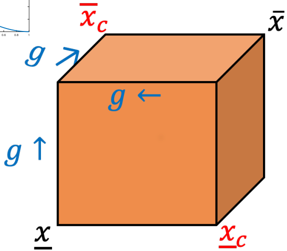
$$\underbrace{H^{\oplus}\underline{x} - H^{\ominus}\overline{x} + g(\underline{x}_c)}_{f_d(\underline{x},\overline{x})} \leq \underbrace{Hx + g(x)}_{f(x)} \leq \underbrace{H^{\oplus}\overline{x} - H^{\ominus}\underline{x} + g(\overline{x}_c)}_{f_d(\overline{x},\underline{x})}$$

Remainder-Form Mixed-Monotone Decompositions

Khajenejad, M. and Yong, S.Z. "Tight Remainder-Form Decomposition Functions with Applications to Constrained Reachability and Guaranteed State Estimation." *IEEE Transactions on Automatic Control*, 2023, accepted, (Impact Factor = 6.549).

$$f(x) = \underbrace{Hx}_{\text{linear remainder}} + \underbrace{g(x)}_{\text{JSS mapping}} \quad , H_{i,j} = \overline{J}^f_{i,j} \vee H_{i,j} = \underline{J}^f_{i,j}$$





$$H^{\oplus}\underline{x} - H^{\ominus}\overline{x} \leq Hx \leq H^{\oplus}\overline{x} - H^{\ominus}\underline{x}$$

$$g(\underline{x}_c) \leq g(x) \leq g(\overline{x}_c)$$

$$\underbrace{H^{\oplus}\underline{x} - H^{\ominus}\overline{x} + g(\underline{x}_c)}_{f_d(\underline{x},\overline{x})} \leq \underbrace{Hx + g(x)}_{f(x)} \leq \underbrace{H^{\oplus}\overline{x} - H^{\ominus}\underline{x} + g(\overline{x}_c)}_{f_d(\overline{x},\underline{x})}$$

Technical Contributions

- no remainder outperforms all linear remainders

- tractable computations; a countable finite set of slopes $\mathcal{H}$

$$\underbrace{\max_{H \in \mathcal{H}} H^{\oplus}\underline{x} - H^{\ominus}\overline{x} + g(\underline{x}_c)}_{\underline{f}_d(\underline{x},\overline{x})} \leq f(x) \leq \underbrace{\min_{H \in \mathcal{H}} H^{\oplus}\overline{x} - H^{\ominus}\underline{x} + g(\overline{x}_c)}_{\overline{f}_d(\overline{x},\underline{x})}$$

- one-sided bounded Jacobians

Technical Contributions

- no remainder outperforms all linear remainders

- tractable computations; a countable finite set of slopes $\mathcal{H}$

$$\underbrace{\max_{H\in\mathcal{H}} H^{\oplus}\underline{x} - H^{\ominus}\overline{x} + g(\underline{x}_c)}_{\underline{f}_d(\underline{x},\overline{x})} \leq f(x) \leq \underbrace{\min_{H\in\mathcal{H}} H^{\oplus}\overline{x} - H^{\ominus}\underline{x} + g(\overline{x}_c)}_{\overline{f}_d(\overline{x},\underline{x})}$$

- one-sided bounded Jacobians

Technical Contributions

- no remainder outperforms all linear remainders

- tractable computations; a countable finite set of slopes $\mathcal{H}$

$$\underbrace{\max_{H\in\mathcal{H}} H^{\oplus}\underline{x} - H^{\ominus}\overline{x} + g(\underline{x}_c)}_{\underline{f}_d(\underline{x},\overline{x})} \leq f(x) \leq \underbrace{\min_{H\in\mathcal{H}} H^{\oplus}\overline{x} - H^{\ominus}\underline{x} + g(\overline{x}_c)}_{\overline{f}_d(\overline{x},\underline{x})}$$

- one-sided bounded Jacobians

Technical Contributions

- nonsmooth systems; generalized Clarke derivatives
- discontinuous vector fields with finite jumps
- outperforms [Yang.ea.2019]

Technical Contributions

- nonsmooth systems; generalized Clarke derivatives
- discontinuous vector fields with finite jumps
- outperforms [Yang.ea.2019]

Technical Contributions

- nonsmooth systems; generalized Clarke derivatives
- discontinuous vector fields with finite jumps
- outperforms [Yang.ea.2019]

Outline; from Mixed-Monotonicity to...

- remainder-form decomposition functions
- applications:
  - set-valued state estimation
  - interval observer design
  - (distributed) resiliency
- future visions

Embedding Systems; Unconstrained Reachability

$$\underbrace{x^+ = f(x,w)}_{\text{original } n\text{-dimensional system}} \longrightarrow \underbrace{\begin{bmatrix}\underline{x}^+ \\ \overline{x}^+\end{bmatrix} = \begin{bmatrix}\underline{f}_d([\underline{x}^\top \ \underline{w}^\top]^\top, [\overline{x}^\top \ \overline{w}^\top]^\top) \\ \overline{f}_d([\overline{x}^\top \ \overline{w}^\top]^\top, [\underline{x}^\top \ \underline{w}^\top]^\top)\end{bmatrix}}_{\text{lifted } 2n\text{-dimensional embedding system}}$$

Proposition 2 (State Framer Property [Khajenejad.Yong.2021])

$$\underline{x}_t \leq x_t \leq \overline{x}_t, \forall t \geq 0, \forall w \in \mathcal{W}.$$

Van Der Pol System

$$\begin{aligned} x_{1,k+1} &= x_{1,k} + \delta_t x_{2,k}, \\ x_{2,k+1} &= x_{2,k} + \delta_t((1 - x_{1,k}^2)x_{2,k} - x_{1,k}) \end{aligned}$$

Embedding Systems; Unconstrained Reachability

$$\underbrace{x^+ = f(x,w)}_{\text{original } n\text{-dimensional system}} \longrightarrow \underbrace{\begin{bmatrix} \underline{x}^+ \\ \overline{x}^+ \end{bmatrix} = \begin{bmatrix} \underline{f}_d([\underline{x}^\top \ \underline{w}^\top]^\top, [\overline{x}^\top \ \overline{w}^\top]^\top) \\ \overline{f}_d([\overline{x}^\top \ \overline{w}^\top]^\top, [\underline{x}^\top \ \underline{w}^\top]^\top) \end{bmatrix}}_{\text{lifted } 2n\text{-dimensional embedding system}}$$

Proposition 2 (State Framer Property [Khajenejad.Yong.2021])

$$\underline{x}_t \leq x_t \leq \overline{x}_t, \forall t \geq 0, \forall w \in \mathcal{W}.$$

Van Der Pol System

$$\begin{aligned} x_{1,k+1} &= x_{1,k} + \delta_t x_{2,k}, \\ x_{2,k+1} &= x_{2,k} + \delta_t((1 - x_{1,k}^2)x_{2,k} - x_{1,k}) \end{aligned}$$

Embedding Systems; Unconstrained Reachability

$$\underbrace{x^+ = f(x, w)}_{\text{original } n\text{-dimensional system}} \quad \longrightarrow \quad \underbrace{\begin{bmatrix} \underline{x}^+ \\ \overline{x}^+ \end{bmatrix} = \begin{bmatrix} \underline{f}_d([\underline{x}^\top \ \underline{w}^\top]^\top, [\overline{x}^\top \ \overline{w}^\top]^\top) \\ \overline{f}_d([\overline{x}^\top \ \overline{w}^\top]^\top, [\underline{x}^\top \ \underline{w}^\top]^\top) \end{bmatrix}}_{\text{lifted } 2n\text{-dimensional embedding system}}$$

Proposition 2 (State Framer Property [Khajenejad.Yong.2021])

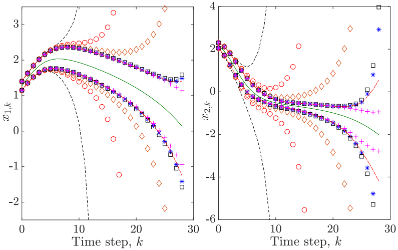
$$\underline{x}_t \le x_t \le \overline{x}_t, \forall t \ge 0, \forall w \in \mathcal{W}.$$

Van Der Pol System

$$\begin{aligned} x_{1,k+1} &= x_{1,k} + \delta_t x_{2,k}, \\ x_{2,k+1} &= x_{2,k} + \delta_t((1 - x_{1,k}^2)x_{2,k} - x_{1,k}) \end{aligned}$$

−−: natural, ○: centered form,
◇: mixed-centered form inclusions
□: [Yang.ea.2019], ∗: **remainder-form**,

·-: the best of all, +: optimal



Set-Inversion; Constrained Reachability

$$x^+ = f(x, w)$$
$$h(x) \in \underbrace{Y = [\underline{y}, \overline{y}]}_{\text{constraint, observation, measurement set}}$$

Problem 5 (Set-Inversion)

Find $[X_u] \supseteq \{x \in [X_p] | h(x) \in Y\}$

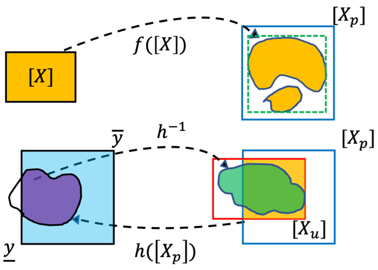
- Fact: $\forall x \in [\underline{x}_m, \overline{x}_m] \subseteq [X_p] \Rightarrow h_d(\underline{x}_m, \overline{x}_m) \leq h(x) \leq h_d(\overline{x}_m, \underline{x}_m)$

$$\begin{cases} h_d(\overline{x}_m, \underline{x}_m) < \underline{y} \\ \quad \text{or} \\ h_d(\underline{x}_m, \overline{x}_m) > \overline{y} \end{cases} ?$$

Set-Inversion; Constrained Reachability

$$x^+ = f(x, w)$$
$$h(x) \in \underbrace{Y = [\underline{y}, \overline{y}]}$$

constraint, observation, measurement set



Problem 5 (Set-Inversion)

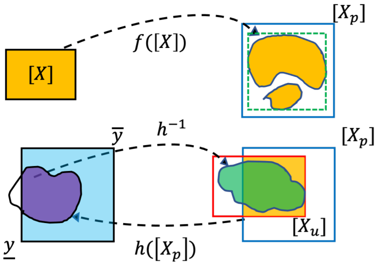
Find $[X_u] \supseteq \{x \in [X_p] | h(x) \in Y\}$

- Fact: $\forall x \in [\underline{x}_m, \overline{x}_m] \subseteq [X_p] \Rightarrow h_d(\underline{x}_m, \overline{x}_m) \leq h(x) \leq h_d(\overline{x}_m, \underline{x}_m)$

$$\begin{cases} h_d(\overline{x}_m, \underline{x}_m) < \underline{y} \\ \text{or} \\ h_d(\underline{x}_m, \overline{x}_m) > \overline{y} \end{cases} ?$$

$$x^+ = f(x, w)$$
$$h(x) \in \underbrace{Y = [\underline{y}, \overline{y}]}$$

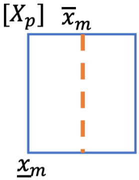
constraint, observation, measurement set



Problem 5 (Set-Inversion)

Find $[X_u] \supseteq \{x \in [X_p] | h(x) \in Y\}$

- Fact: $\forall x \in [\underline{x}_m, \overline{x}_m] \subseteq [X_p] \Rightarrow h_d(\underline{x}_m, \overline{x}_m) \leq h(x) \leq h_d(\overline{x}_m, \underline{x}_m)$

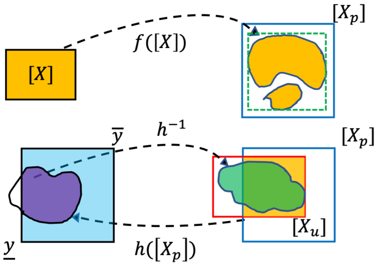


$$\begin{cases} h_d(\overline{x}_m, \underline{x}_m) < \underline{y} \\ \quad\text{or} \\ h_d(\underline{x}_m, \overline{x}_m) > \overline{y} \end{cases} ?$$

Set-Inversion; Constrained Reachability

$$x^+ = f(x, w)$$
$$h(x) \in \underbrace{Y = [\underline{y}, \overline{y}]}$$

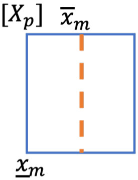
constraint, observation, measurement set



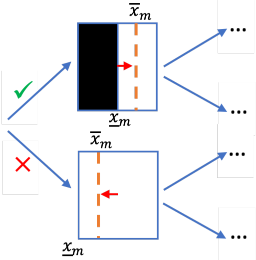
Problem 5 (Set-Inversion)

Find $[X_u] \supseteq \{x \in [X_p] | h(x) \in Y\}$

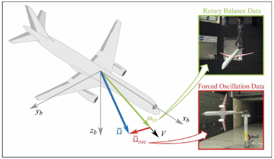
- Fact: $\forall x \in [\underline{x}_m, \overline{x}_m] \subseteq [X_p] \Rightarrow h_d(\underline{x}_m, \overline{x}_m) \leq h(x) \leq h_d(\overline{x}_m, \underline{x}_m)$



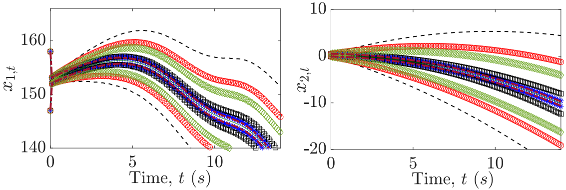
$$\begin{cases} h_d(\overline{x}_m, \underline{x}_m) < \underline{y} \\ \text{or} \\ h_d(\underline{x}_m, \overline{x}_m) > \overline{y} \end{cases} \quad ?$$



NASA's Generic Transport Model [Summers.ea.2013]



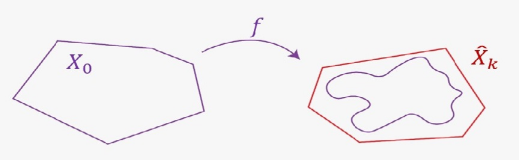
- a remote-controlled commercial aircraft
- V, α, q & θ: speed, angle of attack, pitch rate & pitch angle



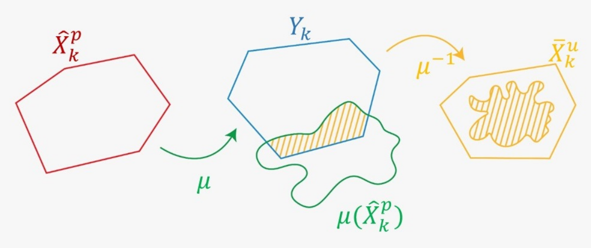
upper and lower framers of $x_1 = v$ and $x_2 = \alpha$, natural ($--$), centered form ($\circ$), $mixed - form$ ($\diamond$), [Yang.ea.2019]($\square$), **remainder-form** ($*$)

Polytopic Estimation

- Can mixed-monotone decomposition be applied for polytope-valued state estimation?

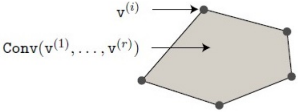


Propagation: $f(X_0) \subseteq \hat{X}_k$

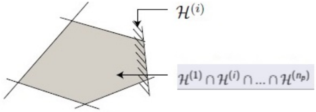


Update: $\hat{X}_k^p \cap_\mu Y_k \subseteq \overline{X}_k^u$

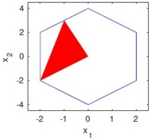
Polytopes; Equivalent Representations

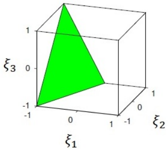


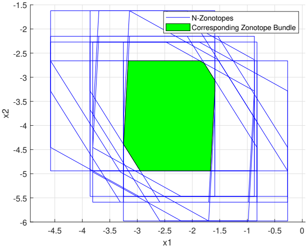
(a) $V - representation$



(b) $H - representation$







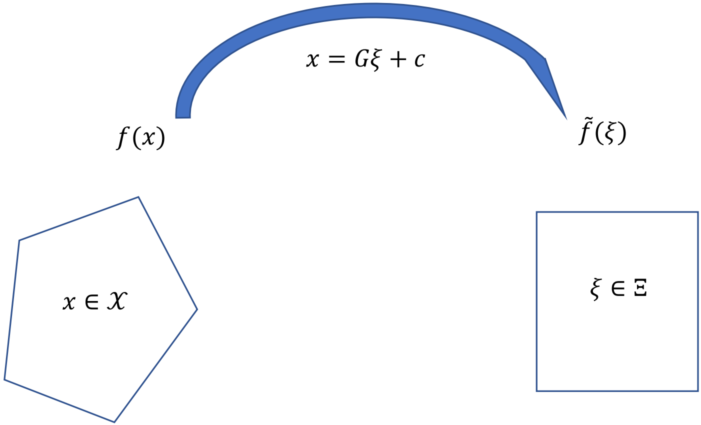
$$\underbrace{\mathcal{Z} = \{\tilde{G}\xi + \tilde{c} | \xi \in \mathbb{B}^{n_g}, \tilde{A}\xi = \tilde{b}\}}_{\text{Constrained Zonotope (CZ)}}$$

$$\underbrace{\mathcal{Z} = \bigcap_{s=1}^{S} \{G_s\zeta + c_s | \zeta \in \mathbb{B}^{\hat{n}_g}\}}_{\text{Zonotope Bundle (ZB)}}$$

Main Idea

Khajenejad, M. and Yong, S.Z. "Guaranteed State Estimation via Direct Polytopic Set Computation for Nonlinear Discrete-Time Systems." *IEEE Control Systems Letters (L-CSS)*, pages 2060–2065, vol. 6, 2022 (presented in ACC'22).

Khajenejad, M., Shoaib, F. and Yong, S.Z. "Guaranteed State Estimation via Indirect Polytopic Set Computation for Nonlinear Discrete-Time Systems." *IEEE Conference on Decision and Control (CDC)*, Austin, Texas (Virtual), pp. 6167–6174, 2021 (average acceptance rate: %56.7).

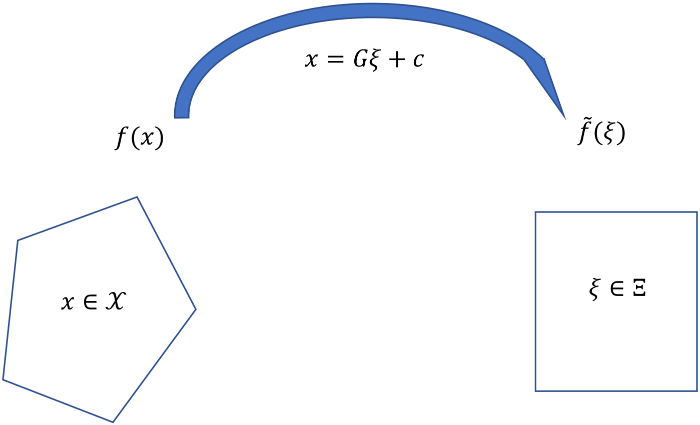


- Now apply mixed-monotone decompositions in the space of generators (Ξ) for propagation and update

Main Idea

Khajenejad, M. and Yong, S.Z. "Guaranteed State Estimation via Direct Polytopic Set Computation for Nonlinear Discrete-Time Systems." *IEEE Control Systems Letters (L-CSS)*, pages 2060–2065, vol. 6, 2022 (presented in ACC'22).

Khajenejad, M., Shoaib, F. and Yong, S.Z. "Guaranteed State Estimation via Indirect Polytopic Set Computation for Nonlinear Discrete-Time Systems." *IEEE Conference on Decision and Control (CDC)*, Austin, Texas (Virtual), pp. 6167–6174, 2021 (average acceptance rate: %56.7).

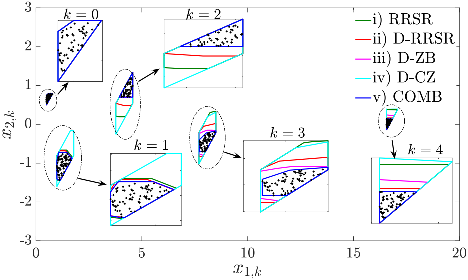


- Now apply mixed-monotone decompositions in the space of generators (Ξ) for propagation and update

Polytope-Valued State Estimation

[Example I, Rego.ea.2020]

$$
\begin{aligned}
x_{1,k} &= 3x_{1,k-1} - \frac{x_{1,k-1}^2}{7} - \frac{4x_{1,k-1}x_{2,k-1}}{4+x_{1,k-1}} + w_{1,k-1},\\
x_{2,k} &= -2x_{2,k-1} + \frac{3x_{1,k-1}x_{2,k-1}}{4+x_{1,k-1}} + w_{2,k-1}, \|w_k\|_\infty \leq 0.1,\\
\begin{bmatrix} y_{1,k} \\ y_{2,k} \end{bmatrix} &= \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x_{1,k} \\ x_{2,k} \end{bmatrix} + \begin{bmatrix} v_{1,k} \\ v_{2,k} \end{bmatrix}, \mathcal{X}_0 = \{\begin{bmatrix} 0.1 & 0.2 & -0.1 \\ 0.1 & 0.1 & 0 \end{bmatrix}, \begin{bmatrix} 0.5 \\ 0.5 \end{bmatrix}\}, \|v_k\|_\infty \leq 0.4,
\end{aligned}
$$



polytopic estimates for five different approaches. **COMB**: combination of the zonotope-bundle (D-ZB) and constrained zonotope (D-CZ) approaches

Outline; from Mixed-Monotonicity to...

- remainder-form decomposition functions

- applications:
  - set-valued state estimation
  - interval observer design
  - (distributed) resiliency

- future visions

Interval Observer Synthesis

- How about stability/boundedness of the framers?

$$\mathcal{G}: \begin{cases} x_t^+ = f(x_t, w_t), \\ y_t = h(x_t, v_t) \end{cases}$$

Problem 6 (Interval Observer Synthesis)

synthesize framers $\underline{x}_t, \overline{x}_t$ such that

- *states are framed: $\underline{x}_t \leq x_t \leq \overline{x}_t$*
- *framers are uniformly bounded*
- *design is optimized*

Interval Observer Synthesis

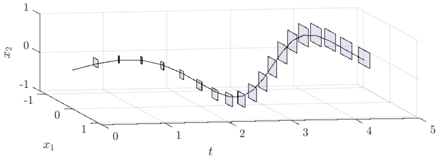
- How about stability/boundedness of the framers?

$$\mathcal{G}: \begin{cases} x_t^+ = f(x_t, w_t), \\ y_t = h(x_t, v_t) \end{cases}$$

Problem 6 (Interval Observer Synthesis)

synthesize framers $\underline{x}_t, \overline{x}_t$ such that

- *states are framed: $\underline{x}_t \leq x_t \leq \overline{x}_t$*
- *framers are uniformly bounded*
- *design is optimized*



Design Strategy: JSS decomposition of vector fields

$$\left.\begin{aligned} x^+ &= f(x,w) = Ax + Bw + \underbrace{\phi(x,w)}_{\text{JSS}} \\ y &= h(x,v) = Cx + Dv + \underbrace{\psi(x,v)}_{\text{JSS}} \\ 0 &= L(y - Cx - Dv - \psi(x,v)) \end{aligned}\right\} \Longrightarrow$$

$$x^+ = \underbrace{(A-LC)x + Bw - LDv}_{f_\ell(\underbrace{x,w,v}_{\xi})} + Ly + \underbrace{\phi(x,w) - L\psi(x,v)}_{f_\nu(\underbrace{x,w,v}_{\xi})}$$

Linear + Nonlinear Embedding Systems

$$\begin{cases} \underline{x}^+ = f_{\ell d}(\underline{\xi},\overline{\xi}) + f_{\nu d}(\underline{\xi},\overline{\xi}) + Ly \\ \overline{x}^+ = f_{\ell d}(\overline{\xi},\underline{\xi}) + f_{\nu d}(\overline{\xi},\underline{\xi}) + Ly \end{cases}$$

Khajenejad, M. and Yong, S.Z. "$\mathcal{H}_\infty$-Optimal Interval Observer Synthesis for Uncertain Nonlinear Dynamical Systems via Mixed-Monotone Decompositions." *IEEE Control Systems Letters (L-CSS)*, pages 3008–3013, vol. 6, 2022 (presented in CDC'22).

Khajenejad, M., Shoaib, F. and Yong, S.Z. "Interval Observer Synthesis for Locally Lipschitz Nonlinear Dynamical Systems via Mixed-Monotone Decompositions." *American Control Conference (ACC)*, Atlanta, Georgia, pp. 2970–2975, 2022 (average acceptance rate: %67).

Pati T., **Khajenejad, M.**, Daddala S.P. and Yong, S.Z. "L_1-Robust Interval Observer Design for Uncertain Nonlinear Dynamical Systems." *IEEE Control Systems Letters (L-CSS)*, pages 3475–3480, vol. 6, 2022 (presented in CDC'22).

Design Strategy: JSS decomposition of vector fields

$$\left.\begin{aligned} x^+ &= f(x,w) = Ax + Bw + \underbrace{\phi(x,w)}_{\text{JSS}} \\ y &= h(x,v) = Cx + Dv + \underbrace{\psi(x,v)}_{\text{JSS}} \\ 0 &= L(y - Cx - Dv - \psi(x,v)) \end{aligned}\right\} \Longrightarrow$$

$$x^+ = \underbrace{(A - LC)x + Bw - LDv}_{f_\ell(\underbrace{x,w,v}_{\xi})} + Ly + \underbrace{\phi(x,w) - L\psi(x,v)}_{f_\nu(\underbrace{x,w,v}_{\xi})}$$

Linear + Nonlinear Embedding Systems

$$\begin{cases} \underline{x}^+ = f_{\ell d}(\underline{\xi}, \overline{\xi}) + f_{\nu d}(\underline{\xi}, \overline{\xi}) + Ly \\ \overline{x}^+ = f_{\ell d}(\overline{\xi}, \underline{\xi}) + f_{\nu d}(\overline{\xi}, \underline{\xi}) + Ly \end{cases}$$

Khajenejad, M. and Yong, S.Z. "$\mathcal{H}_\infty$-Optimal Interval Observer Synthesis for Uncertain Nonlinear Dynamical Systems via Mixed-Monotone Decompositions." *IEEE Control Systems Letters (L-CSS)*, pages 3008–3013, vol. 6, 2022 (presented in CDC'22).

Khajenejad, M., Shoaib, F. and Yong, S.Z. "Interval Observer Synthesis for Locally Lipschitz Nonlinear Dynamical Systems via Mixed-Monotone Decompositions." *American Control Conference (ACC)*, Atlanta, Georgia, pp. 2970–2975, 2022 (average acceptance rate: %67).

Pati T., **Khajenejad, M.**, Daddala S.P. and Yong, S.Z. "L_1-Robust Interval Observer Design for Uncertain Nonlinear Dynamical Systems." *IEEE Control Systems Letters (L-CSS)*, pages 3475–3480, vol. 6, 2022 (presented in CDC'22).

Design Strategy: JSS decomposition of vector fields

$$\left.\begin{aligned} x^+ &= f(x,w) = Ax + Bw + \underbrace{\phi(x,w)}_{\text{JSS}} \\ y &= h(x,v) = Cx + Dv + \underbrace{\psi(x,v)}_{\text{JSS}} \\ 0 &= L(y - Cx - Dv - \psi(x,v)) \end{aligned}\right\} \Longrightarrow$$

$$x^+ = \underbrace{(A-LC)x + Bw - LDv}_{f_\ell(\underbrace{x,w,v}_{\xi})} + Ly + \underbrace{\phi(x,w) - L\psi(x,v)}_{f_\nu(\underbrace{x,w,v}_{\xi})}$$

Linear + Nonlinear Embedding Systems

$$\begin{cases} \underline{x}^+ = f_{\ell d}(\underline{\xi}, \overline{\xi}) + f_{\nu d}(\underline{\xi}, \overline{\xi}) + Ly \\ \overline{x}^+ = f_{\ell d}(\overline{\xi}, \underline{\xi}) + f_{\nu d}(\overline{\xi}, \underline{\xi}) + Ly \end{cases}$$

Khajenejad, M. and Yong, S.Z. "$\mathcal{H}_\infty$-Optimal Interval Observer Synthesis for Uncertain Nonlinear Dynamical Systems via Mixed-Monotone Decompositions." *IEEE Control Systems Letters (L-CSS)*, pages 3008–3013, vol. 6, 2022 (presented in CDC'22).

Khajenejad, M., Shoaib, F. and Yong, S.Z. "Interval Observer Synthesis for Locally Lipschitz Nonlinear Dynamical Systems via Mixed-Monotone Decompositions." *American Control Conference (ACC)*, Atlanta, Georgia, pp. 2970–2975, 2022 (average acceptance rate: %67).

Pati T., **Khajenejad, M.**, Daddala S.P. and Yong, S.Z. "L_1-Robust Interval Observer Design for Uncertain Nonlinear Dynamical Systems." *IEEE Control Systems Letters (L-CSS)*, pages 3475–3480, vol. 6, 2022 (presented in CDC'22).

Theorem 1 (ISS & $\mathcal{H}_\infty/L_1$-Optimal Observer Design)

- *locally Lipschitz ⇒ mixed-monotonicity ⇒ embedding systems*
- *SDP/MILP ⇒ $\mathcal{H}_\infty/L_1$-optimal gains*
- *both continuous-time and discrete-time systems*

Theorem 1 (ISS & $\mathcal{H}_\infty/L_1$-Optimal Observer Design)

- *locally Lipschitz ⇒ mixed-monotonicity ⇒ embedding systems*
- *SDP/MILP ⇒ $\mathcal{H}_\infty/L_1$-optimal gains*
- *both continuous-time and discrete-time systems*

Observer Synthesis

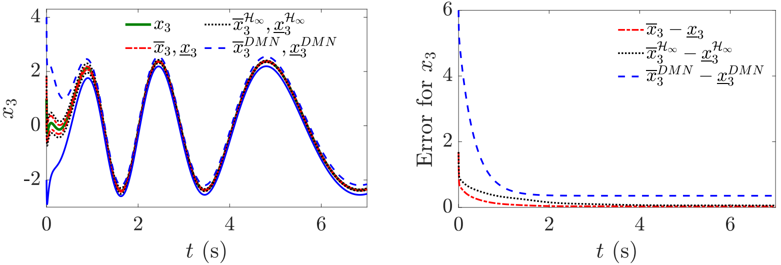
Theorem 1 (ISS & $\mathcal{H}_\infty/L_1$-Optimal Observer Design)

- *locally Lipschitz ⇒ mixed-monotonicity ⇒ embedding systems*
- *SDP/MILP ⇒ $\mathcal{H}_\infty/L_1$-optimal gains*
- *both continuous-time and discrete-time systems*

Simulation Results

[CT Example, Dinh.ea.2014]

$$\dot{x}_1 = x_2 + w_1, \quad \dot{x}_2 = b_1 x_3 - a_1 \sin(x_1) - a_2 x_2 + w_2,$$
$$\dot{x}_3 = -a_2 a_3 x_1 + \frac{a_1}{b_1}(a_4 \sin(x_1) + \cos(x_1) x_2) - a_3 x_2 - a_4 x_3 + w_3, \quad y = x_1.$$

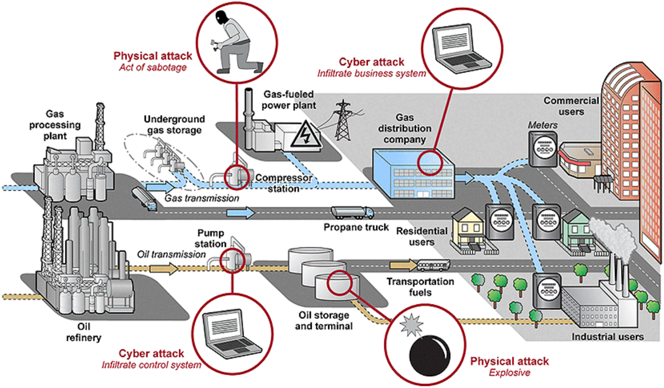


State, x_3, as well as its upper and lower framers and error returned by our proposed $L_!$ observer, $\overline{x}_3, \underline{x}_3$, our proposed $\mathcal{H}_\infty$ observer, $\overline{x}_3^{\mathcal{H}_\infty}, \underline{x}_3^{\mathcal{H}_\infty}$, and by the observer in [Dinh.ea.2014], $\overline{x}_3^{DMN}, \underline{x}_3^{DMN}, \varepsilon_3^{DMN}$.

Outline; from Mixed-Monotonicity to...

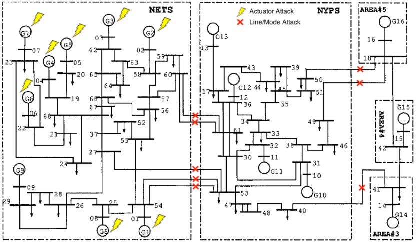
- remainder-form decomposition functions
- applications:
  - set-valued state estimation
  - interval observer design
  - (distributed) resiliency
- future visions

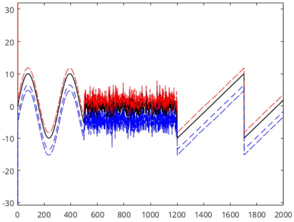
Data Attack Resiliency



- Can we simultaneously obtain guaranteed estimates of states and unknown inputs (adversarial signals) and possibly mitigate their effect?

Resilient Observer Design; State and Input Estimation



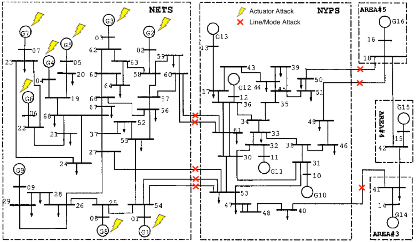


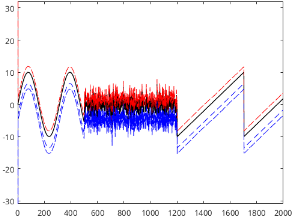
$$x_{k+1} = f(x_k) + Bu_k + Ww_k + Gd_k,$$
$$y_k = h(x_k) + D\underbrace{u_k}_{\text{known, control input}} + Vv_k + H\underbrace{d_k}_{\text{unknown input}}$$

- no prior 'useful' knowledge or assumption or known bounds on the dynamics of d_k

Problem 7 (Simultaneous Input and State Observer)

design stable and optimal set-valued input and state estimates





$$x_{k+1} = f(x_k) + Bu_k + Ww_k + Gd_k,$$
$$y_k = h(x_k) + \underbrace{D\,u_k}_{\text{known, control input}} + Vv_k + H\,\underbrace{d_k}_{\text{unknown input}}$$

- no prior 'useful' knowledge or assumption or known bounds on the dynamics of d_k

Problem 7 (Simultaneous Input and State Observer)

design stable and optimal set-valued input and state estimates

Design Strategy: Unknown Input Decomposition

$$x_{k+1} = f(x_k) + Bu_k + Gd_k + Ww_k,$$
$$y_k = h(x_k) + Du_k + Hd_k + Vv_k$$

Key Insights:

- $d_k \Leftrightarrow d_{1,k}$ & $d_{2,k}$:
- $y_k \Leftrightarrow z_{1,k}$ & $z_{2,k}$:
- auxiliary state: $\gamma_k \triangleq \Lambda(I - NC_2)x_k$
  - unaffected by d_k
- $\Lambda(I - NC_2)(f(x) - G_1 S h_1(x)) = \underbrace{Ax + \rho(x)}_{\text{mixed-monotone decomposition}}$
- $L(z_{2,k} - C_2 x_k - \psi_2(x_k) - V_2 v_k) = 0$

Design Strategy: Unknown Input Decomposition

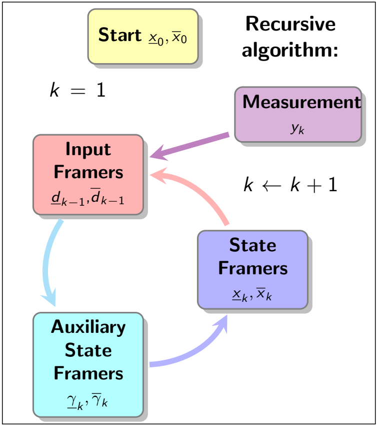
$$\begin{aligned} x_{k+1} &= f(x_k) + Bu_k + G_1 d_{1,k} + G_2 d_{2,k} + Ww_k, \\ z_{1,k} &= h_1(x_k) + \Sigma d_{1,k} + D_1 u_k + V_1 v_k \\ z_{2,k} &= \underbrace{C_2 x_k + \psi_2(x_k)}_{\text{mixed-monotone decomposition}} + D_2 u_k + V_2 v_k \end{aligned}$$

Key Insights:

- $d_k \Leftrightarrow d_{1,k}$ & $d_{2,k}$:
- $y_k \Leftrightarrow z_{1,k}$ & $z_{2,k}$:
- auxiliary state: $\gamma_k \triangleq \Lambda(I - NC_2)x_k$
  - unaffected by d_k
- $\Lambda(I - NC_2)(f(x) - G_1 S h_1(x)) = \underbrace{Ax + \rho(x)}_{\text{mixed-monotone decomposition}}$
- $L(z_{2,k} - C_2 x_k - \psi_2(x_k) - V_2 v_k) = 0$

Design Strategy: Unknown Input Decomposition

$$
\begin{aligned}
x_{k+1} &= f(x_k) + Bu_k + G_1 d_{1,k} + G_2 d_{2,k} + Ww_k, \\
z_{1,k} &= h_1(x_k) + \Sigma d_{1,k} + D_1 u_k + V_1 v_k \\
z_{2,k} &= \underbrace{C_2 x_k + \psi_2(x_k)}_{\text{mixed-monotone decomposition}} + D_2 u_k + V_2 v_k
\end{aligned}
$$



Key Insights:

- $d_k \Leftrightarrow d_{1,k}$ & $d_{2,k}$:
- $y_k \Leftrightarrow z_{1,k}$ & $z_{2,k}$:
- auxiliary state: $\gamma_k \triangleq \Lambda(I - NC_2)x_k$
  - unaffected by d_k
- $\Lambda(I - NC_2)(f(x) - G_1 S h_1(x)) = \underbrace{Ax + \rho(x)}_{\text{mixed-monotone decomposition}}$
- $L(z_{2,k} - C_2 x_k - \psi_2(x_k) - V_2 v_k) = 0$

3-Step Recursive Observer

Input Framer Computation

$$\begin{aligned}\underline{d}_{k-1} &= \Phi^{\oplus}\underline{x}_k - \Phi^{\ominus}\overline{x}_k + J_d(\underline{x}_{k-1},\overline{x}_{k-1}) + A_z z_{1,k-1} \\ &+A_v^{\oplus}\underline{v} - A_v^{\ominus}\overline{v} + \Phi^{\ominus}\underline{w} - \Phi^{\oplus}\overline{w}, \\ \overline{d}_{k-1} &= \Phi^{\oplus}\overline{x}_k - \Phi^{\ominus}\underline{x}_k + J_d(\overline{x}_{k-1},\underline{x}_{k-1}) + A_z z_{1,k-1} \\ &+A_v^{\oplus}\overline{v} - A_v^{\ominus}\underline{v} + \Phi^{\ominus}\overline{w} - \Phi^{\oplus}\underline{w},\end{aligned}$$

Auxiliary State Propagation

$$\begin{aligned}\underline{\gamma}_{k+1} &= (A-LC_2)^{\oplus}\underline{\gamma}_k - (A-LC_2)^{\ominus}\overline{\gamma}_k + \rho_d(\underline{x}_k,\overline{x}_k) \\ &+D^{\ominus}\underline{\epsilon} - D^{\oplus}\overline{\epsilon} + L^{\ominus}\psi_{2,d}(\underline{x}_k,\overline{x}_k) - L^{\oplus}\psi_{2,d}(\overline{x}_k,\underline{x}_k) \\ &+\hat{V}^{\ominus}\underline{v} - \hat{V}^{\oplus}\overline{v} + \hat{W}^{\ominus}\underline{w} - \hat{W}^{\ominus}\overline{w} + \hat{z}_k, \\ \overline{\gamma}_{k+1} &= (A-LC_2)^{\oplus}\overline{\gamma}_k - (A-LC_2)^{\ominus}\underline{\gamma}_k + \rho_d(\overline{x}_k,\underline{x}_k) \\ &+D^{\ominus}\overline{\epsilon} - D^{\oplus}\underline{\epsilon} + L^{\ominus}\psi_{2,d}(\overline{x}_k,\underline{x}_k) - L^{\oplus}\psi_{2,d}(\underline{x}_k,\overline{x}_k) \\ &+\hat{V}^{\ominus}\overline{v} - \hat{V}^{\oplus}\underline{v} + \hat{W}^{\oplus}\overline{w} - \hat{W}^{\ominus}\underline{w} + \hat{z}_k,\end{aligned}$$

State Framer Computation

$$\begin{aligned}\underline{x}_k &= \underline{\gamma}_k + \Lambda N z_{2,k} + \Lambda^{\ominus}\underline{\epsilon} - \Lambda^{\oplus}\overline{\epsilon} + (\Lambda N V_2)^{\ominus}\underline{v} - (\Lambda N V_2)^{\oplus}\overline{v}, \\ \overline{x}_k &= \overline{\gamma}_k + \Lambda N z_{2,k} + \Lambda^{\ominus}\overline{\epsilon} - \Lambda^{\oplus}\underline{\epsilon} + (\Lambda N V_2)^{\ominus}\overline{v} - (\Lambda N V_2)^{\oplus}\underline{v},\end{aligned}$$

$\mathcal{H}_\infty$-Optimal State and Input Observer Design

Error Dynamics

$$
\begin{aligned}
e^x_{k+1} \leq\; & (|A - LC_2| + \overline{F}_\rho + |L|\overline{F}_{\psi_2})e^x_k + |\hat{W}|\delta^w \\
& +(|V_a - LV_b| - |A - LC_2||\Lambda N V_2| + |\Lambda N V_2|)\delta^v \\
& +(|\Lambda| + |D_a - LD_b| - |A - LC_2||\Lambda|)\delta^\epsilon,
\end{aligned}
$$

Theorem 2 ($\mathcal{H}_\infty$-Observer Design)

- *strong observability* $\Longrightarrow$ *existence of decompositions*
- *semi-definite programs* $\Longrightarrow$ *optimal stabilizing gains*
- *various comparison systems* $\Longrightarrow$ *various sufficient conditions*

Khajenejad, M., Jin, Z., Dinh T.N. and Yong, S.Z. "Resilient State Estimation for Nonlinear Discrete-Time Systems via Input and State Interval Observer Synthesis." *IEEE Conference on Decision and Control (CDC)*, 2023, under review.

$\mathcal{H}_\infty$-Optimal State and Input Observer Design

Error Dynamics

$$
\begin{aligned}
e^x_{k+1} \leq\ & (|A - LC_2| + \overline{F}_\rho + |L|\overline{F}_{\psi_2})e^x_k + |\hat{W}|\delta^w \\
& +(|V_a - LV_b| - |A - LC_2||\Lambda N V_2| + |\Lambda N V_2|)\delta^v \\
& +(|\Lambda| + |D_a - LD_b| - |A - LC_2||\Lambda|)\delta^\epsilon,
\end{aligned}
$$

Theorem 2 ($\mathcal{H}_\infty$-Observer Design)

- *strong observability* $\Longrightarrow$ *existence of decompositions*
- *semi-definite programs* $\Longrightarrow$ *optimal stabilizing gains*
- *various comparison systems* $\Longrightarrow$ *various sufficient conditions*

Khajenejad, M., Jin, Z., Dinh T.N. and Yong, S.Z. "Resilient State Estimation for Nonlinear Discrete-Time Systems via Input and State Interval Observer Synthesis." *IEEE Conference on Decision and Control (CDC)*, 2023, under review.

$\mathcal{H}_\infty$-Optimal State and Input Observer Design

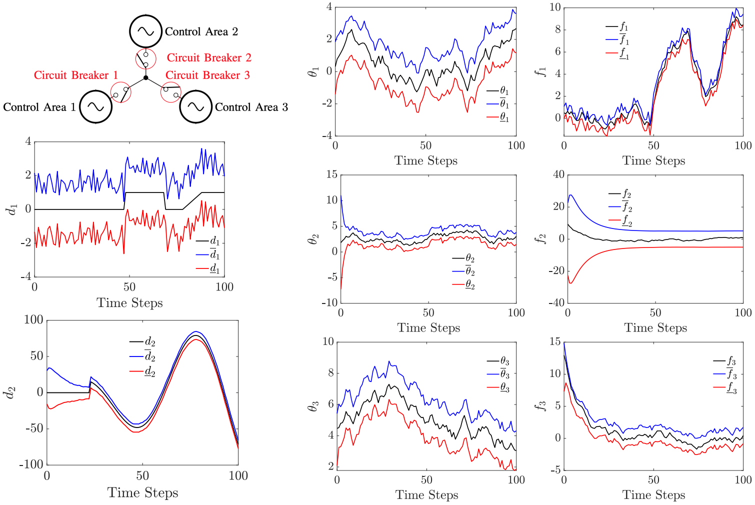
Error Dynamics

$$
\begin{aligned}
e^x_{k+1} \leq\ & (|A - LC_2| + \overline{F}_\rho + |L|\overline{F}_{\psi_2})e^x_k + |\hat{W}|\delta^w \\
& +(|V_a - LV_b| - |A - LC_2||\Lambda N V_2| + |\Lambda N V_2|)\delta^v \\
& +(|\Lambda| + |D_a - LD_b| - |A - LC_2||\Lambda|)\delta^\epsilon,
\end{aligned}
$$

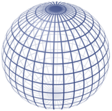
Theorem 2 ($\mathcal{H}_\infty$-Observer Design)

- *strong observability* $\Longrightarrow$ *existence of decompositions*
- *semi-definite programs* $\Longrightarrow$ *optimal stabilizing gains*
- *various comparison systems* $\Longrightarrow$ *various sufficient conditions*

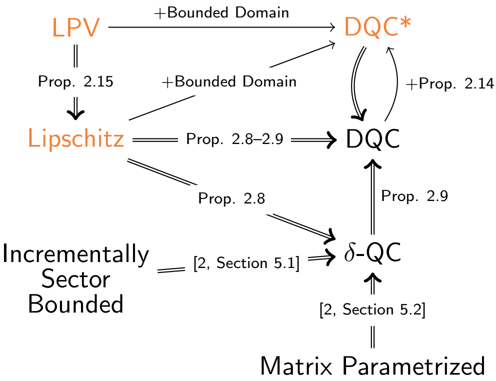
Khajenejad, M., Jin, Z., Dinh T.N. and Yong, S.Z. "Resilient State Estimation for Nonlinear Discrete-Time Systems via Input and State Interval Observer Synthesis." *IEEE Conference on Decision and Control (CDC)*, 2023, under review.


Control Area 2
Circuit Breaker 2
Circuit Breaker 1
Circuit Breaker 3
Control Area 1
Control Area 3
Time Steps

Resilient Hyperball-Valued Observers



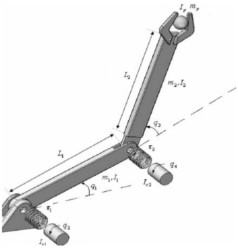
$$\begin{cases} \|x_k - \hat{x}_k\|_2 \leq \delta_k^x \\ \|d_{k-1} - \hat{d}_{k-1}\|_2 \leq \delta_{k-1}^d \end{cases}$$

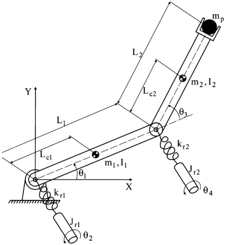


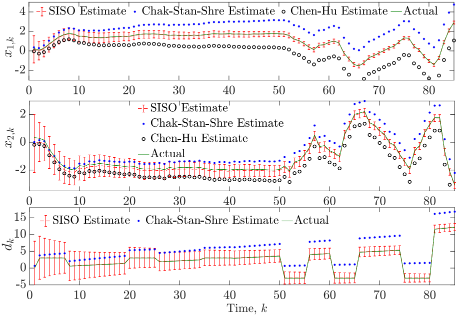
Khajenejad, M. and Yong, S.Z. "Simultaneous Input and State Set-Valued $\mathcal{H}_\infty$-Observers For Linear Parameter-Varying Systems." *American Control Conference (ACC)*, Philadelphia, PA, pp. 4521–4526, 2019.

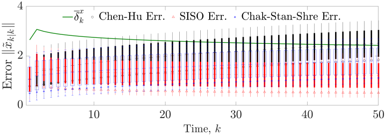
Khajenejad, M. and Yong, S.Z. "Simultaneous State and Unknown Input Set-Valued Observers for Quadratically Constrained Nonlinear Dynamical Systems." *International Journal of Robust and Nonlinear Control*, pages 6589–6622, vol. 32, issue 12, 2022 (Impact Factor = 3.897).

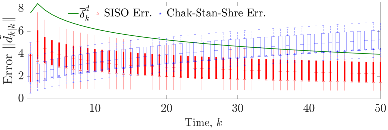
Simulation Results: Two-Link Flexible-Joint Robot











Scalable & Distributed Resiliency in CPS

Target system, $x \in \mathbb{R}^n$

$$x^+ = f(x, w, d)$$

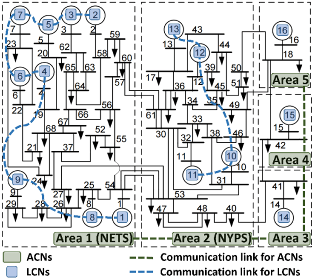
$$w \in [\underline{w}, \overline{w}], \; d \in \mathbb{R}^p$$

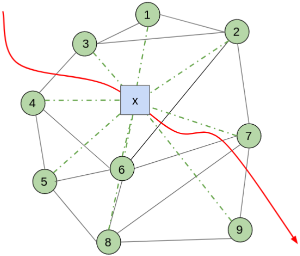
d is unknown and arbitrary

Sensor network, $i = 1, \dots, N$

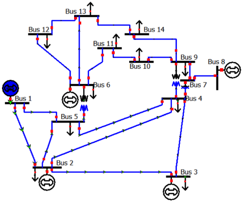
$$y^i = h^i(x, v^i, d), \; v^i \in [\underline{v}^i, \overline{v}^i]$$

collective positive detectability





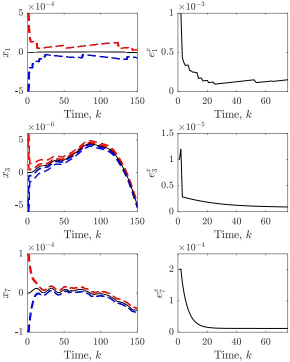
Distributed Set-Valued Input & State Observer Design

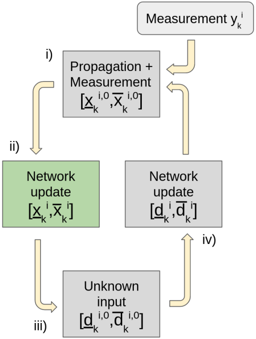


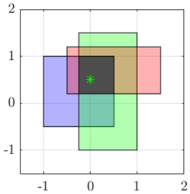
Network update: min/max consensus

$$\underline{x}_k^{i,t} = \max_{j \in \mathcal{N}_i} \underline{x}_k^{j,t-1} \qquad \overline{x}_k^{i,t} = \min_{j \in \mathcal{N}_i} \overline{x}_k^{j,t-1}$$

$$\underline{x}_k^{i} = \underline{x}_k^{i,t_x} \qquad \overline{x}_k^{i} = \overline{x}_k^{i,t_x}$$







DARPA

Khajenejad, M., Brown, S., and Martínez, S. "Distributed Interval Observers for LTI Systems with Bounded Noise." *American Control Conference (ACC)*, San Diego, California, accepted, 2023 (average acceptance rate: %67).

Khajenejad, M., Brown, S., and Martínez, S. "Distributed Resilient Interval Observers for Bounded-Error LTI Systems Subject to False Data Injection Attacks ." *American Control Conference (ACC)*, San Diego, California, accepted, 2023 (average acceptance rate: %67).

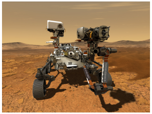
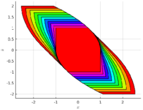
Takeaway

$$\begin{cases} \text{mixed-monotonicity} \\ \\ \text{strong detectability} \\ \\ \text{collective positive detectability} \end{cases} \overset{\checkmark}{\Longrightarrow} \begin{cases} \text{robust reachability} \\ \\ \text{attack mitigation} \\ \\ \text{distributed resiliency} \end{cases}$$

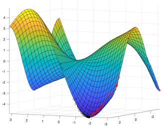
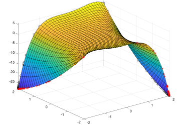
Outline; from Mixed-Monotonicity to...

- remainder-form decomposition functions
- applications:
  - set-valued state estimation
  - interval observer design
  - (distributed) resiliency
- future visions

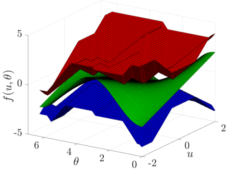
Towards Hybrid, Nonconvex & Unknown CPS

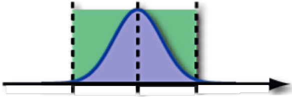
hybrid reachability and invariance properties

nonconvex optimization



unknown CPS: set-membership learning meets model-based approaches

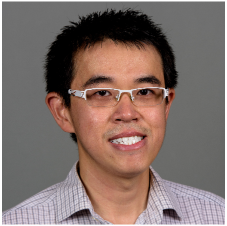


aleatoric+epistemic uncertainties: random sets

- NSF-CPS, NASA-NSPIRES early career award

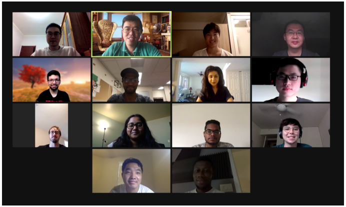
Thank you! Questions?

Taha, Fatemeh, Marsa



Sze Zheng Yong

Sonia Martinez



My labmates

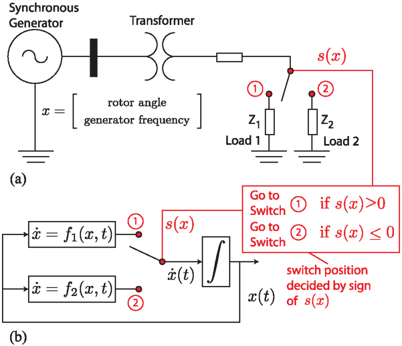
Ira A. Fulton Schools of Engineering
Arizona State University

UC San Diego
Jacobs School of Engineering

Back-Up Slides

Mode (Switching) Attack Resiliency

- How about if we have switching attacks, as well?



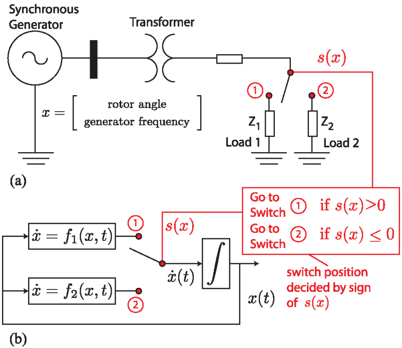
- q: discrete switching unknown mode of the system, modified by switching attacks

Switched (Non)linear Discrete-time System

$$x_{k+1} = f^q(x_k) + B^q u_k^q + G^q d_k^q + W^q w_k^q,$$
$$y_k = C^q x_k + D^q u_k^q + H^q d_k^q + v_k^q, \quad q \in \mathbb{Q}.$$

Mode (Switching) Attack Resiliency

- How about if we have switching attacks, as well?



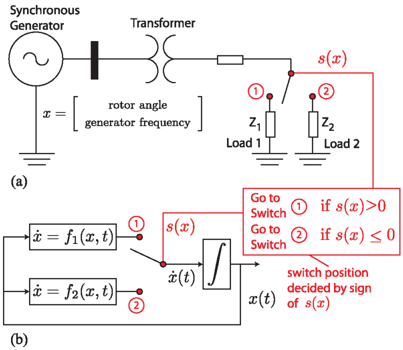
- q: discrete switching unknown mode of the system, modified by switching attacks

Switched (Non)linear Discrete-time System

$$x_{k+1} = f^q(x_k) + B^q u_k^q + G^q d_k^q + W^q w_k^q,$$
$$y_k = C^q x_k + D^q u_k^q + H^q d_k^q + v_k^q, \quad q \in \mathbb{Q}.$$

Mode (Switching) Attack Resiliency

- How about if we have switching attacks, as well?

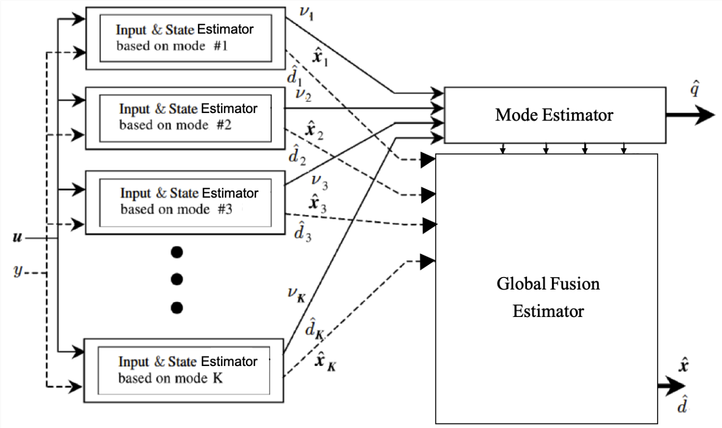


- q: discrete switching unknown mode of the system, modified by switching attacks

Switched (Non)linear Discrete-time System

$$
\begin{aligned}
x_{k+1} &= f^q(x_k) + B^q u_k^q + G^q d_k^q + W^q w_k^q, \\
y_k &= C^q x_k + D^q u_k^q + H^q d_k^q + v_k^q, \quad q \in \mathbb{Q}.
\end{aligned}
$$

Multiple-Model Framework



Khajenejad, M. and Yong, S.Z. "Resilient State Estimation and Attack Mitigation in Cyber-Physical Systems." *Security and Resilience in Cyber-Physical Systems: Detection, Estimation and Control*, Springer, pages 149–185, 2022.

Khajenejad, M. and Yong, S.Z. "Simultaneous Mode, State and Input Set-Valued Observers for Switched Nonlinear Systems." *Automatica*, 2022, under review.

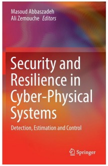
Khajenejad, M. and Yong, S.Z. "Simultaneous Mode, Input and State Set-Valued Observers with Applications to Resilient Estimation against Sparse Attacks." *IEEE Conference on Decision and Control (CDC)*, Nice, France, pp. 1544–1550, 2019 (average acceptance rate: %56.7).

Mode Detectability

- Adversarial property serves as an additional sensor

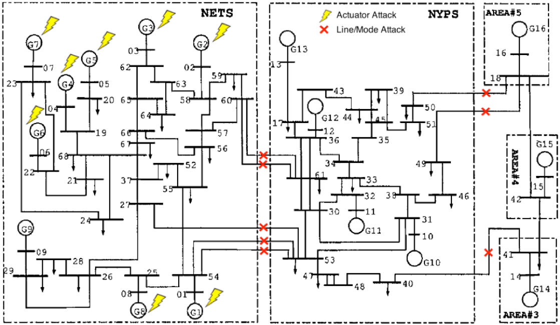
Theorem 8 (Sufficient Conditions for Mode Detectability)

All false modes are eliminated if the unknown input signal has unlimited energy.



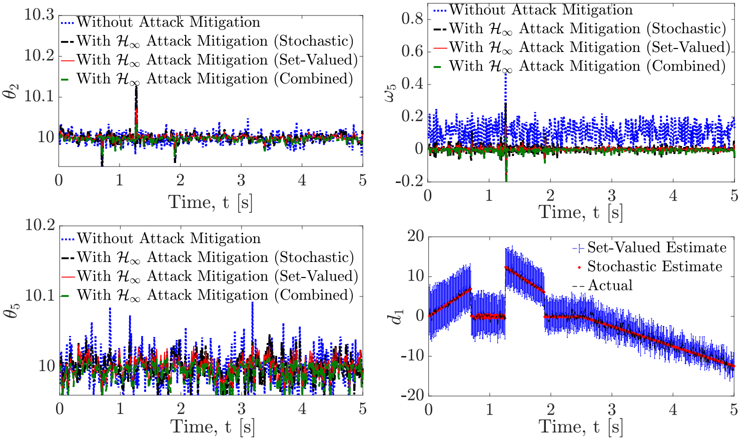
Khajenejad, M. and Yong, S.Z. "Resilient State Estimation and Attack Mitigation in Cyber-Physical Systems." *Security and Resilience in Cyber-Physical Systems: Detection, Estimation and Control*, Springer, pages 149–185, 2022.

Resilient Estimation and Attack Mitigation in CPS



IEEE 68-bus test system with locations of potential actuator signal and mode/transmission line attacks ($n = 136$).

Resilient Estimation and Attack Mitigation in CPS



A comparison of system states with and without the proposed attack mitigation, as well as the attack signal and its point-valued (stochastic) and set-valued (bounded-error) estimates

Definition 9 (Embedding Systems)

- $x_t^+ = f(x_t, w_t)$: an n-dimensional DT/CT system
- $x_0 \in [\underline{x}_0 \ \overline{x}_0]$, $w_t \in [\underline{w} \ \overline{w}]$
- $f_d(\cdot, \cdot)$: any decomposition function of f
- $2n$-dimensional embedding system:

$$\begin{bmatrix} \underline{x}_t^+ \\ \overline{x}_t^+ \end{bmatrix} = \begin{bmatrix} f_d([\underline{x}_t^\top \ \underline{w}^\top]^\top, [\overline{x}_t^\top \ \overline{w}^\top]^\top) \\ f_d([\overline{x}_t^\top \ \overline{w}^\top]^\top, [\underline{x}_t^\top \ \underline{w}^\top]^\top) \end{bmatrix} \tag{2}$$

Proposition 3 (State Framer Property [Khajenejad.Yong.2021])

$$\underline{x}_t \leq x_t \leq \overline{x}_t, \forall t \geq 0, \forall w \in \mathcal{W}.$$

Definition 9 (Embedding Systems)

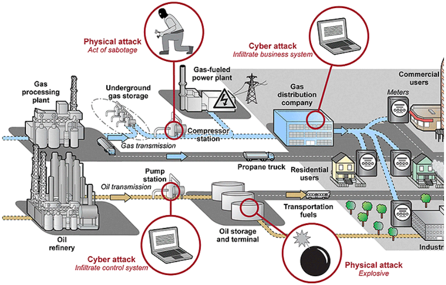
- $x_t^+ = f(x_t, w_t)$: an n-dimensional DT/CT system
- $x_0 \in [\underline{x}_0 \ \overline{x}_0]$, $w_t \in [\underline{w} \ \overline{w}]$
- $f_d(\cdot, \cdot)$: any decomposition function of f
- $2n$-dimensional embedding system:

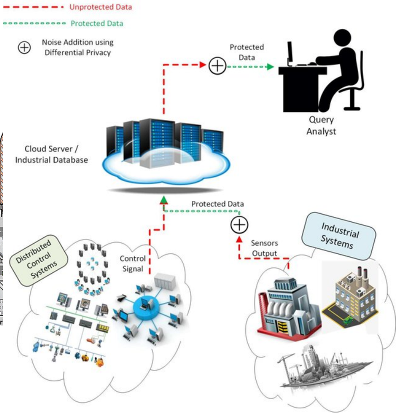
$$\begin{bmatrix} \underline{x}_t^+ \\ \overline{x}_t^+ \end{bmatrix} = \begin{bmatrix} f_d([\underline{x}_t^\top \ \underline{w}^\top]^\top, [\overline{x}_t^\top \ \overline{w}^\top]^\top) \\ f_d([\overline{x}_t^\top \ \overline{w}^\top]^\top, [\underline{x}_t^\top \ \underline{w}^\top]^\top) \end{bmatrix} \quad (2)$$

Proposition 3 (State Framer Property [Khajenejad.Yong.2021])

$$\underline{x}_t \leq x_t \leq \overline{x}_t, \forall t \geq 0, \forall w \in \mathcal{W}.$$

Future Vision: 1. Resiliency Meets Privacy



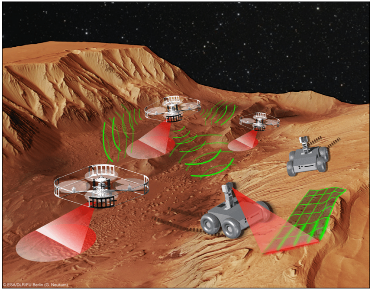


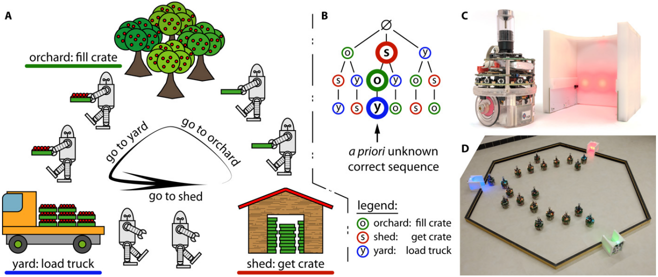
- adversary can **both** inject attack and steal valuable data
- to simultaneously mitigate attacks and protect data
- level of tolerance
- ONR (science of autonomy program), NSF-RI

Khajenejad, M. and Martínez, S. "Guaranteed Privacy of Distributed Nonconvex Optimization via Mixed-Monotone Functional Perturbations." *IEEE Control Systems Letters (L-CSS)*, pages 1081–1086, vol. 7, 2023 (will be presented in ACC'23).

Future Vision: 2. Heterogeneous and Strategic Agents

- heterogeneous beliefs/types
- bounded rationality
- strategic vs. best worst-case
- local communication
- robust dynamic/differential networked games
- ARL, DARPA-ARC, AFOSR-YIP





"Resilient Distributed Learning for Multi-Agent Cooperative Control"

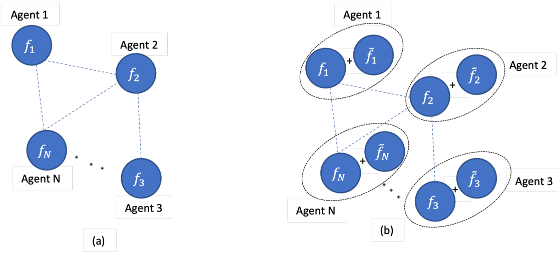
Guaranteed Private Distributed Optimization

Distributed nonconvex optimization

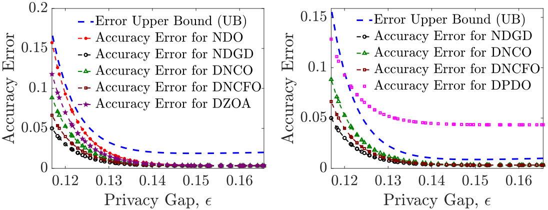
$$\min_{x \in \mathcal{X}_0} f(x) \triangleq \sum_{i=1}^{N} f_i(x),$$

Mixed-monotone functional perturbation

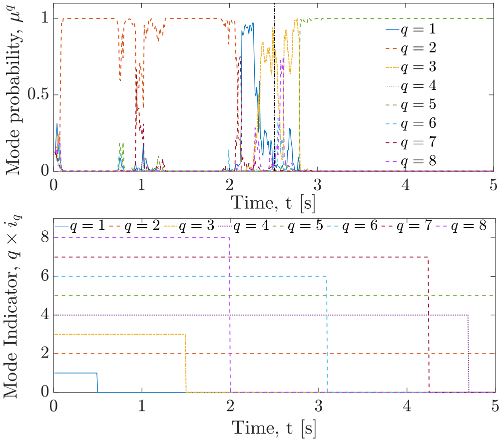
$$g(x) \triangleq \sum_{i=1}^{N} f_i(x) + \overbrace{\tilde{m}_i x}^{\text{unknown, deterministic}}$$



(a) true objective, (b) perturbed objective



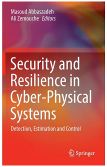
Khajenejad, M. and Martínez, S. "Guaranteed Privacy of Distributed Nonconvex Optimization via Mixed-Monotone Functional Perturbations." *IEEE Control Systems Letters (L-CSS)*, pages 1081–1086, vol. 7, 2023 (will be presented in ACC'23).

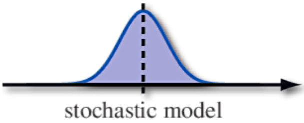


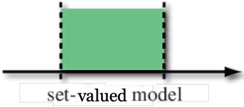
Estimates of mode probabilities when the attack mode switches from $q = 2$ to $q = 5$ at 2.5s assuming stochastic uncertainties, as well as mode indicators assuming bounded norm uncertainties

From
Collective Positive Detectability
to
Distributed Resiliency

Stochastic vs Set-Valued







1. optimality
2. mode detectability
3. attack unidentifiability
4. attack-mitigating

- asymptotic
- maximum likelihood
- Gaussian signal
- $\mathcal{H}_\infty$ controller

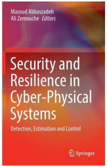
- $\mathcal{H}_\infty$
- elimination
- limited energy
- $\mathcal{H}_\infty$ controller

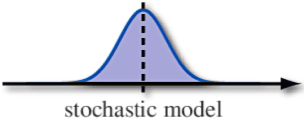
maximum number of (asymptotically) correctable signal attacks

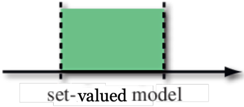
maximum required number of mode/models for estimation resilience

Khajenejad, M. and Yong, S.Z. "Resilient State Estimation and Attack Mitigation in Cyber-Physical Systems." *Security and Resilience in Cyber-Physical Systems: Detection, Estimation and Control*, Springer, pages 149–185, 2022.

Stochastic vs Set-Valued







1. optimality
2. mode detectability
3. attack unidentifiability
4. attack-mitigating

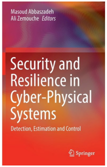
- asymptotic
- maximum likelihood
- Gaussian signal
- $\mathcal{H}_\infty$ controller

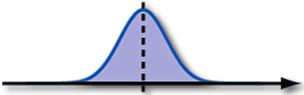
- $\mathcal{H}_\infty$
- elimination
- limited energy
- $\mathcal{H}_\infty$ controller

maximum number of (asymptotically) correctable signal attacks

maximum required number of mode/models for estimation resilience

Khajenejad, M. and Yong, S.Z. "Resilient State Estimation and Attack Mitigation in Cyber-Physical Systems." *Security and Resilience in Cyber-Physical Systems: Detection, Estimation and Control*, Springer, pages 149–185, 2022.





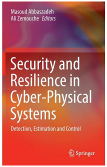
1. optimality
2. mode detectability
3. attack unidentifiability
4. attack-mitigating

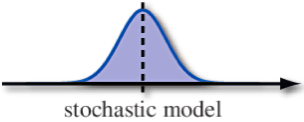
- asymptotic
- maximum likelihood
- Gaussian signal
- $\mathcal{H}_\infty$ controller

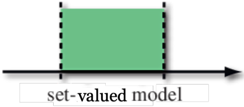
- $\mathcal{H}_\infty$
- elimination
- limited energy
- $\mathcal{H}_\infty$ controller

Khajenejad, M. and Yong, S.Z. "Resilient State Estimation and Attack Mitigation in Cyber-Physical Systems." *Security and Resilience in Cyber-Physical Systems: Detection, Estimation and Control*, Springer, pages 149–185, 2022.

Stochastic vs Set-Valued







1. optimality
2. mode detectability
3. attack unidentifiability
4. attack-mitigating

- asymptotic
- maximum likelihood
- Gaussian signal
- $\mathcal{H}_\infty$ controller

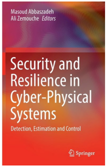
- $\mathcal{H}_\infty$
- elimination
- limited energy
- $\mathcal{H}_\infty$ controller

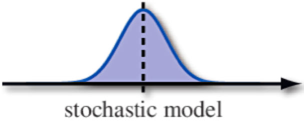
Fundamental limitations

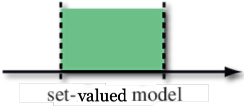
- maximum number of (asymptotically) correctable signal attacks
- maximum required number of mode/models for estimation resilience

Khajenejad, M. and Yong, S.Z. "Resilient State Estimation and Attack Mitigation in Cyber-Physical Systems." *Security and Resilience in Cyber-Physical Systems: Detection, Estimation and Control*, Springer, pages 149–185, 2022.

Stochastic vs Set-Valued







1. optimality
2. mode detectability
3. attack unidentifiability
4. attack-mitigating

- asymptotic
- maximum likelihood
- Gaussian signal
- $\mathcal{H}_\infty$ controller

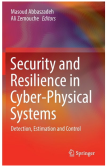
- $\mathcal{H}_\infty$
- elimination
- limited energy
- $\mathcal{H}_\infty$ controller

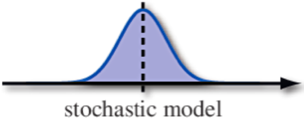
Fundamental limitations

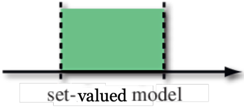
- maximum number of (asymptotically) correctable signal attacks
- maximum required number of mode/models for estimation resilience

Khajenejad, M. and Yong, S.Z. "Resilient State Estimation and Attack Mitigation in Cyber-Physical Systems." *Security and Resilience in Cyber-Physical Systems: Detection, Estimation and Control*, Springer, pages 149–185, 2022.

Stochastic vs Set-Valued







1. optimality
2. mode detectability
3. attack unidentifiability
4. attack-mitigating

- asymptotic
- maximum likelihood
- Gaussian signal
- $\mathcal{H}_\infty$ controller

- $\mathcal{H}_\infty$
- elimination
- limited energy
- $\mathcal{H}_\infty$ controller

Fundamental limitations

- maximum number of (asymptotically) correctable signal attacks
- maximum required number of mode/models for estimation resilience

Khajenejad, M. and Yong, S.Z. "Resilient State Estimation and Attack Mitigation in Cyber-Physical Systems." *Security and Resilience in Cyber-Physical Systems: Detection, Estimation and Control*, Springer, pages 149–185, 2022.

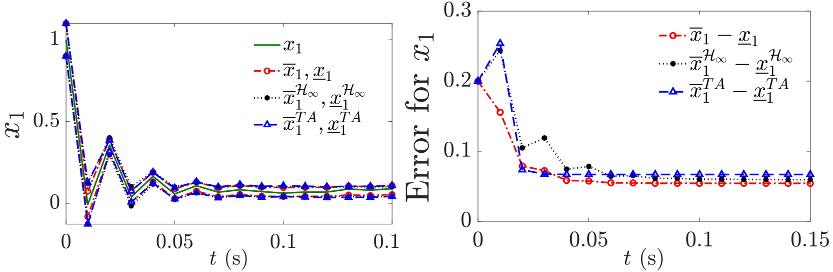
From Strong Detectability to Resiliency

Simulation Results

[DT Example, Hénon Chaos System in Efimov.ea.2013]

$$x_{t+1} = Ax_t + r[1 - x_{t,1}^2] + w_t, \quad y_t = x_{t,1} + v_t,$$

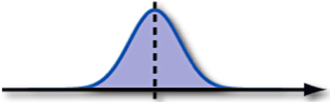
$$A = \begin{bmatrix} 0 & 1 \\ 0.3 & 0 \end{bmatrix},\ r = \begin{bmatrix} 0.05 \\ 0 \end{bmatrix},\ \mathcal{X}_0 = [-2,2] \times [-1,1],\ \mathcal{W} = 0.01[-1,1]^2,\ \mathcal{V} = [-0.1, 0.1].$$



State, x_1, and its upper and lower framers and errors, returned by our proposed observer, $\overline{x}_1, \underline{x}_1$, our proposed $\mathcal{H}_\infty$ observer, $\overline{x}_1^{\mathcal{H}_\infty}, \underline{x}_1^{\mathcal{H}_\infty}$, and by the observer in [Tahir.Açıkmeşe.2021], $\overline{x}_1^{TA}, \underline{x}_1^{TA}$.

From Mixed-Monotonicity to Robustness

Uncertainty Models

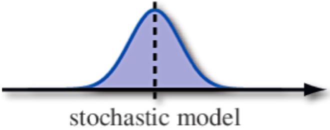


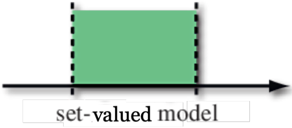
stochastic model

- has distribution
- mean, variance, ...
- expected values
- point estimates
- Kalman filter

- no/unknown distribution
- center, radius, volume, ...
- best worst-case scenario
- set estimates
- set-valued analysis

Uncertainty Models



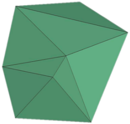


- has distribution
- mean, variance, ...
- expected values
- point estimates
- Kalman filter

- no/unknown distribution
- center, radius, volume, ...
- best worst-case scenario
- set estimates
- set-valued analysis

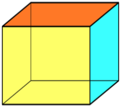
Sets: Examples

$x \in \{x | Ax \leq b\}$



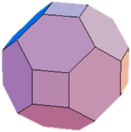
Polytope

$\|u\|_\infty \leq c$



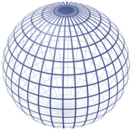
Hyperbox

$w \in \{c + G\xi | \|\xi\|_\infty \leq d\}$

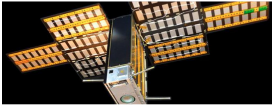


Zonotope

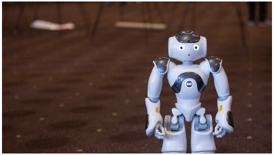
$\|u\|_2 \leq e$



Hyperball



NewSpace Initiative



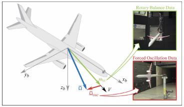
Center for Complex System Safety

Why ASU?

New Economy Initiative

Global Security Initiative

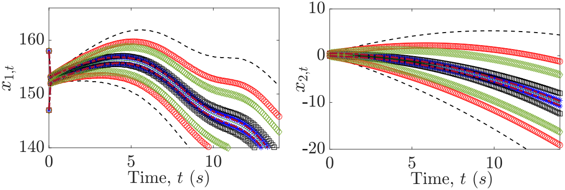
New American University



NASA's Generic Transport Model [Summers.ea.2013]

$$\dot{V} = \frac{-D - mg\sin(\theta-\alpha) + T_x\cos\alpha + T_z\sin\alpha}{m},$$
$$\dot{\alpha} = q + \frac{-L + mg\cos(\theta-\alpha) - T_x\sin\alpha + T_z\cos\alpha}{mV},$$
$$\dot{q} = \frac{M+T_m}{I_{yy}}, \dot{\theta} = q,$$

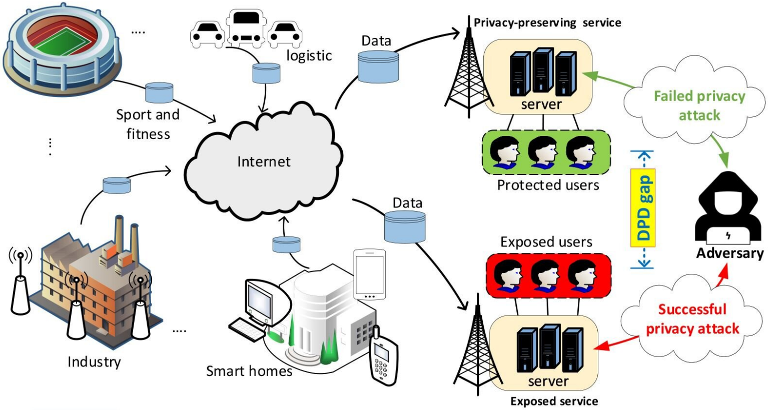
- A remote-controlled commercial aircraft
- V, α, q and θ: air speed, angle of attack, pitch rate and pitch angle



Upper and lower framers of $x_1 = v$ and $x_2 = \alpha$, $T_N(--)$, T_C ($\circ$), T_M ($\diamond$), T_L ($\Box$), T_R ($*$), the best of T_N–T_R (·-), as well as the midpoint trajectory (–).

From Mixed-Monotonicity to Guaranteed Privacy

Privacy

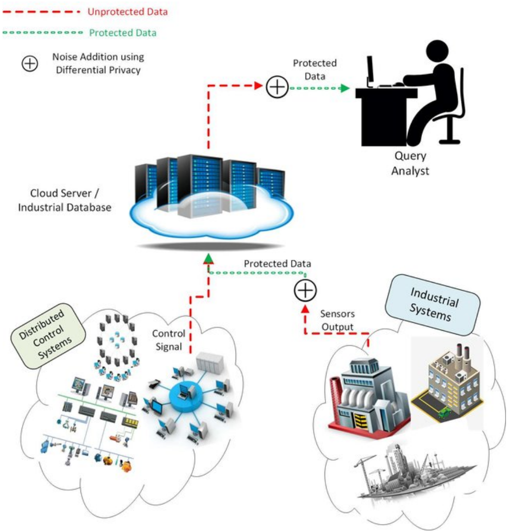


- How can we protect valuable data, identity, info?

Privacy

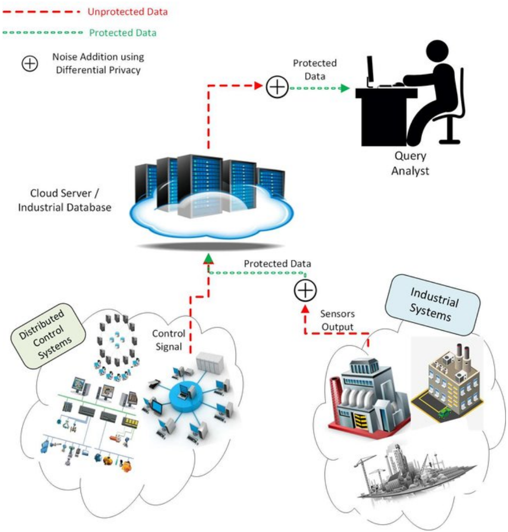
- differential privacy
  - random pert.
  - performance loss
  - stochastic accuracy
- encryption-based
  - comp. overhead
- functional perturbation
  - stochastic guarantee
  - limited func. space
  - convex problems
- hard bounds + nonconvexity

$$\Downarrow$$



Privacy

- differential privacy
  - random pert.
  - performance loss
  - stochastic accuracy
- encryption-based
  - comp. overhead
- functional perturbation
  - stochastic guarantee
  - limited func. space
  - convex problems

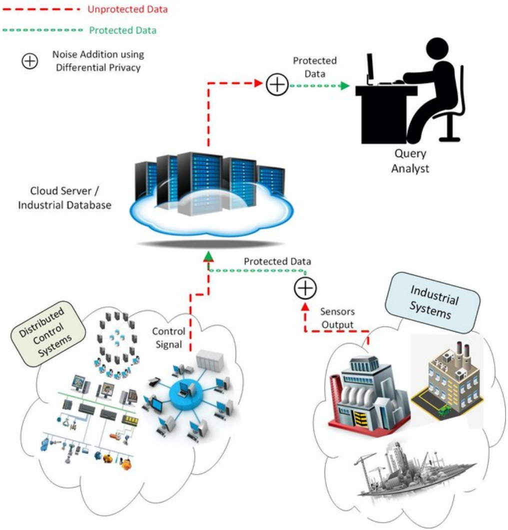


Privacy

- differential privacy
  - random pert.
  - performance loss
  - stochastic accuracy
- encryption-based
  - comp. overhead
- functional perturbation
  - stochastic guarantee
  - limited func. space
  - convex problems
- hard bounds + nonconvexity

⇓

guaranteed privacy

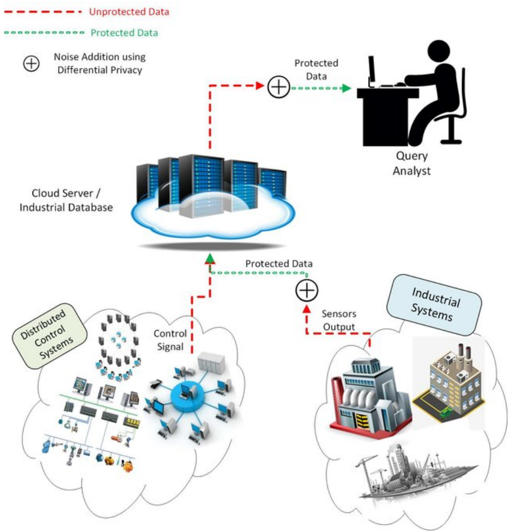


Privacy

- differential privacy
  - random pert.
  - performance loss
  - stochastic accuracy
- encryption-based
  - comp. overhead
- functional perturbation
  - stochastic guarantee
  - limited func. space
  - convex problems
- hard bounds + nonconvexity

$$\Downarrow$$

guaranteed privacy

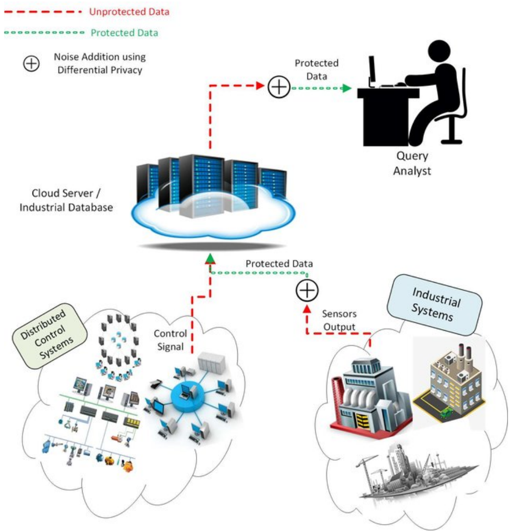


Privacy

- differential privacy
  - random pert.
  - performance loss
  - stochastic accuracy
- encryption-based
  - comp. overhead
- functional perturbation
  - stochastic guarantee
  - limited func. space
  - convex problems
- hard bounds + nonconvexity

$\Downarrow$

guaranteed privacy



Guaranteed Private Distributed Optimization

Distributed nonconvex optimization

$$\min_{x \in \mathcal{X}_0} f(x) \triangleq \sum_{i=1}^{N} f_i(x),$$

Mixed-monotone functional perturbation

$$g(x) \triangleq \sum_{i=1}^{N} f_i(x) + \overbrace{\tilde{m}_i x}^{\text{unknown, deterministic}}$$

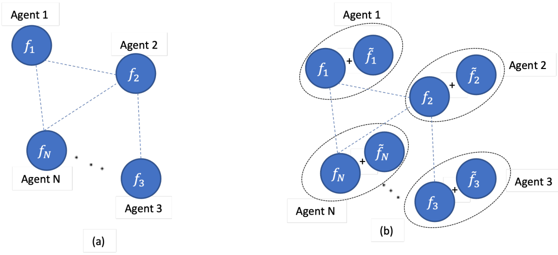
Khajenejad, M. and Martínez, S. "Guaranteed Privacy of Distributed Nonconvex Optimization via Mixed-Monotone Functional Perturbations." *IEEE Control Systems Letters (L-CSS)*, pages 1081–1086, vol. 7, 2023 (will be presented in ACC'23).

Distributed nonconvex optimization

$$\min_{x \in \mathcal{X}_0} f(x) \triangleq \sum_{i=1}^{N} f_i(x),$$

Mixed-monotone functional perturbation

$$g(x) \triangleq \sum_{i=1}^{N} f_i(x) + \overbrace{\tilde{m}_i x}^{\text{unknown, deterministic}}$$



(a) true objective, (b) perturbed objective

Khajenejad, M. and Martínez, S. "Guaranteed Privacy of Distributed Nonconvex Optimization via Mixed-Monotone Functional Perturbations." *IEEE Control Systems Letters (L-CSS)*, pages 1081–1086, vol. 7, 2023 (will be presented in ACC'23).

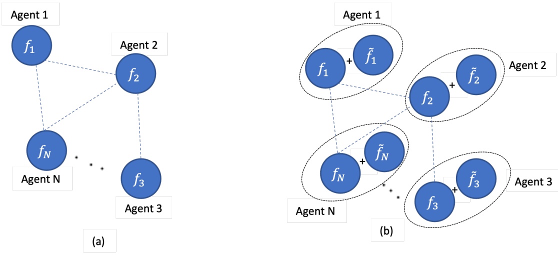
Guaranteed Private Distributed Optimization

Distributed nonconvex optimization

$$\min_{x \in \mathcal{X}_0} f(x) \triangleq \sum_{i=1}^{N} f_i(x),$$

Mixed-monotone functional perturbation

$$g(x) \triangleq \sum_{i=1}^{N} f_i(x) + \overbrace{\tilde{m}_i x}^{\text{unknown, deterministic}}$$



(a) true objective, (b) perturbed objective

Khajenejad, M. and Martínez, S. "Guaranteed Privacy of Distributed Nonconvex Optimization via Mixed-Monotone Functional Perturbations." *IEEE Control Systems Letters (L-CSS)*, pages 1081–1086, vol. 7, 2023 (will be presented in ACC'23).

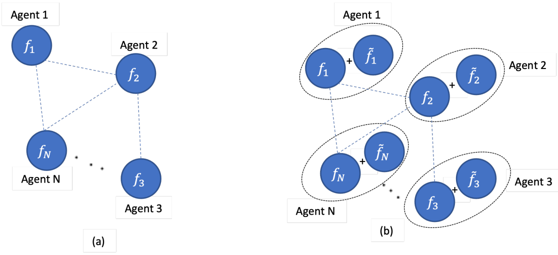
Guaranteed Private Distributed Optimization

Distributed nonconvex optimization

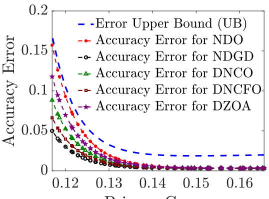
$$\min_{x\in\mathcal{X}_0} f(x) \triangleq \sum_{i=1}^{N} f_i(x),$$

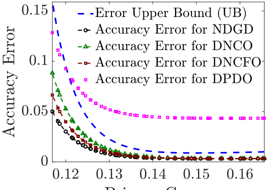
Mixed-monotone functional perturbation

$$g(x)\triangleq\sum_{i=1}^{N} f_i(x)+\overbrace{\tilde{m}_i x}^{\text{unknown, deterministic}}$$



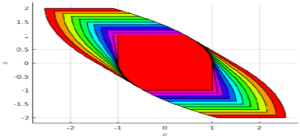
(a) true objective, (b) perturbed objective



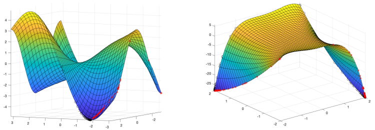


Khajenejad, M. and Martínez, S. "Guaranteed Privacy of Distributed Nonconvex Optimization via Mixed-Monotone Functional Perturbations." *IEEE Control Systems Letters (L-CSS)*, pages 1081–1086, vol. 7, 2023 (will be presented in ACC'23).

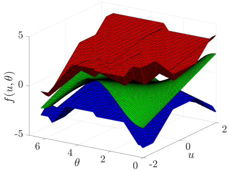
Future Vision: 3. Mixed-Monotonicity; Other interesting Implications



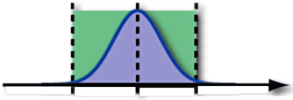
hybrid reachability and invariance properties



nonconvex optimization



unknown CPS: set-membership learning meets model-based approaches



aleatoric+epistemic uncertainties: random sets

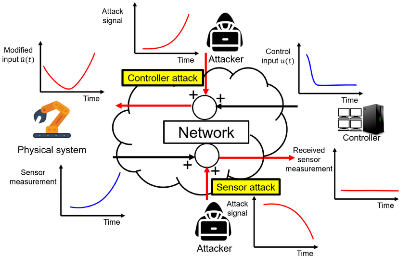
- to target: NSF-CPS, NASA early career award

Past Research

- Input reconstruction and state estimation play key roles in fault detection, attack mitigation, safe control, etc.

Past Research

- Input reconstruction and state estimation play key roles in fault detection, attack mitigation, safe control, etc.

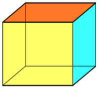


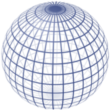
mixed-monotonicity, observability $\Downarrow$ strong detectability, sparsity

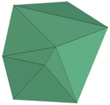
Objective

To simultaneously estimate " sets" of states and unknown inputs and possibly mitigate the effect of attacks

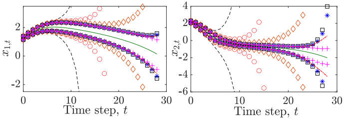
Past Research Overview: Set-Valued Methods



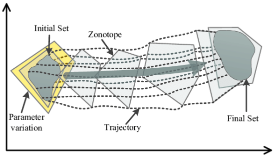




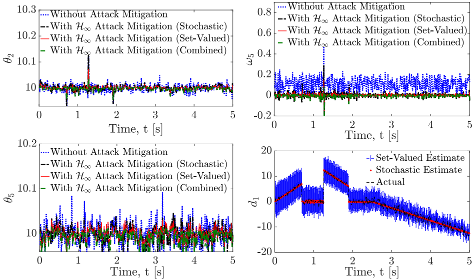
Distribution-free uncertainty sets



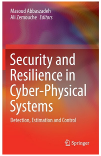
Robust reachability analysis



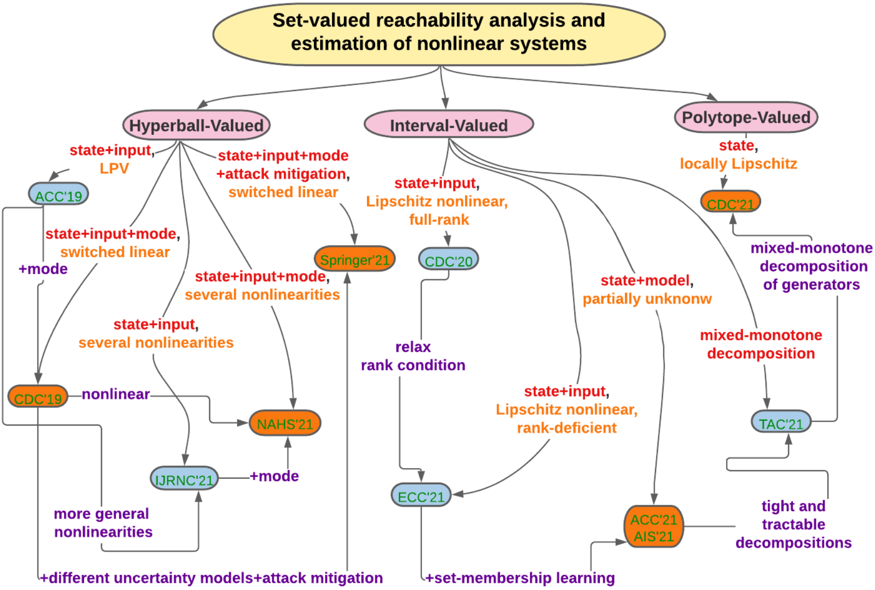
Polytope-valued estimation



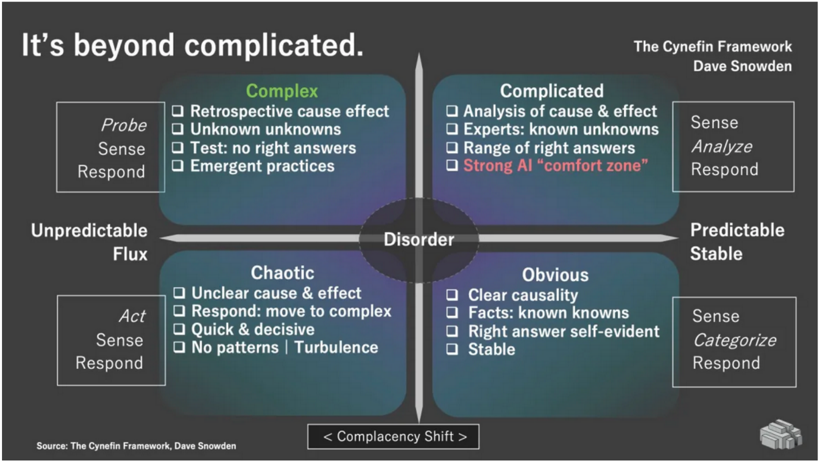
State estimation and attack mitigation



Past Research Roadmap



Perspective



Funding Opportuinities

- NSF CAREER Award ($500k / 5 years)
  - All assistant profs, up to 3 attempts
- Army Research Lab (ARL)
- DoD Young Investigator Programs ($500k / 3 years)
  - AFOSR, ONR, ARO
  - Assistant profs within 5 years of PhD
- DoE Early Career Award ($750k / 5 years)
  - Assistant profs within 10 years of PhD
- DARPA Young Faculty Award ($300k / 2 years)
  - Assistant profs within 10 years of PhD
- NASA Early Career Faculty Award ($600k / 3 years)
- Industry grants (Google, Amazon, Ford, Toyota, etc.)
- ASU New Economy Initiative Science and Technology Centers

Decomposition-Based Set-Inversion Algorithm

- Given μ and $[\underline{y}, \overline{y}]$, find a tight superset of $\{z | \mu(z) \in [\underline{y}, \overline{y}]\}$
- Idea: $z \in [\underline{z}_m, \overline{z}_m] \Rightarrow \mu_d(\underline{z}_m, \overline{z}_m) \leq \mu(z) \leq \mu_d(\overline{z}_m, \underline{z}_m)$
- If $\mu_d(\overline{z}_m, \underline{z}_m) < \underline{y}$ or $\mu_d(\underline{z}_m, \overline{z}_m) > \overline{y}$, then rule out $[\underline{z}_m, \overline{z}_m]$
- Bisection procedure:

Decomposition-Based Set-Inversion Algorithm

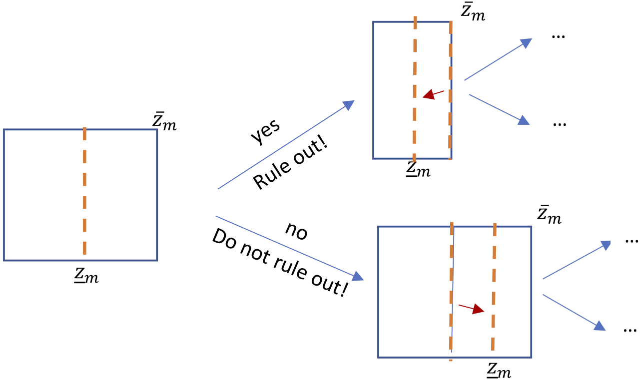
- Given μ and $[\underline{y}, \overline{y}]$, find a tight superset of $\{z | \mu(z) \in [\underline{y}, \overline{y}]\}$
- Idea: $z \in [\underline{z}_m, \overline{z}_m] \Rightarrow \mu_d(\underline{z}_m, \overline{z}_m) \leq \mu(z) \leq \mu_d(\overline{z}_m, \underline{z}_m)$
- If $\mu_d(\overline{z}_m, \underline{z}_m) < \underline{y}$ or $\mu_d(\underline{z}_m, \overline{z}_m) > \overline{y}$, then rule out $[\underline{z}_m, \overline{z}_m]$
- Bisection procedure:

Decomposition-Based Set-Inversion Algorithm

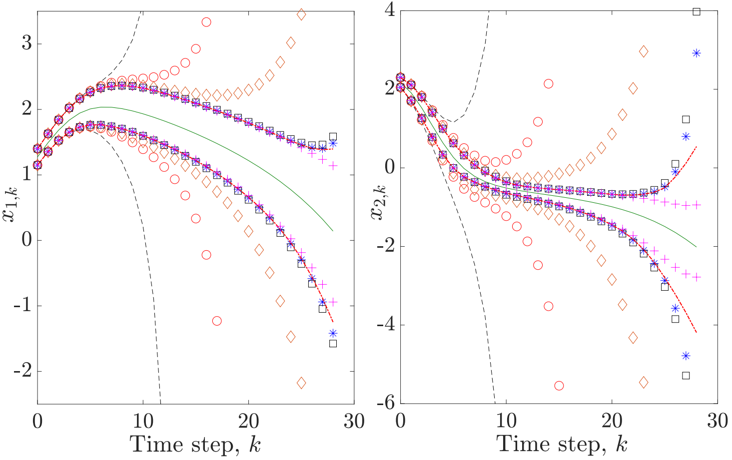
- Given μ and $[\underline{y}, \overline{y}]$, find a tight superset of $\{z|\mu(z) \in [\underline{y}, \overline{y}]\}$
- Idea: $z \in [\underline{z}_m, \overline{z}_m] \Rightarrow \mu_d(\underline{z}_m, \overline{z}_m) \leq \mu(z) \leq \mu_d(\overline{z}_m, \underline{z}_m)$
- If $\mu_d(\overline{z}_m, \underline{z}_m) < \underline{y}$ or $\mu_d(\underline{z}_m, \overline{z}_m) > \overline{y}$, then rule out $[\underline{z}_m, \overline{z}_m]$
- Bisection procedure:

Decomposition-Based Set-Inversion Algorithm

- Given μ and $[\underline{y}, \overline{y}]$, find a tight superset of $\{z | \mu(z) \in [\underline{y}, \overline{y}]\}$
- Idea: $z \in [\underline{z}_m, \overline{z}_m] \Rightarrow \mu_d(\underline{z}_m, \overline{z}_m) \leq \mu(z) \leq \mu_d(\overline{z}_m, \underline{z}_m)$
- If $\mu_d(\overline{z}_m, \underline{z}_m) < \underline{y}$ or $\mu_d(\underline{z}_m, \overline{z}_m) > \overline{y}$, then rule out $[\underline{z}_m, \overline{z}_m]$
- Bisection procedure:



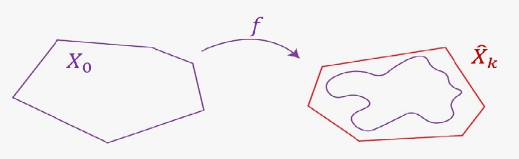
Example: Reachable Sets for Van Der Pol System



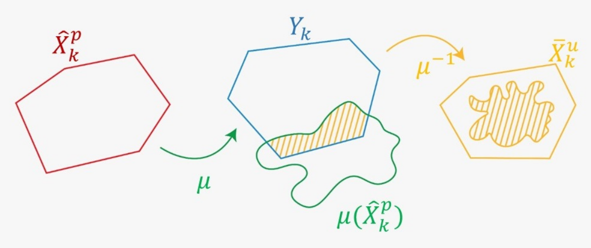
Upper and lower bounds on x_1 and x_2 in Van der Pol system, applying T_N(−−), T_C (○), T_M (◇), T_L (□), T_R (∗), the best of T_N–T_R (·-) and T_O (+), as well as the center trajectory (−).

Polytopic Estimation

- Can mixed-monotone decomposition be applied for polytope-valued state estimation? (CDC'21)

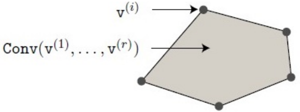


Propagation: $f(X_0) \subseteq \hat{X}_k$

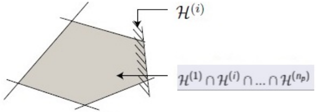


Update: $\hat{X}_k^p \bigcap_{\mu} Y_k \subseteq \overline{X}_k^u$

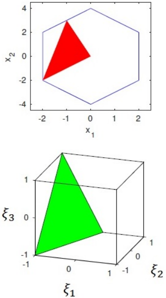
Polytopes; Equivalent Representations

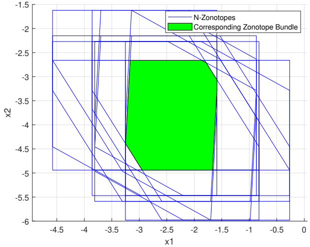


(a) $V - representation$



(b) $H - representation$

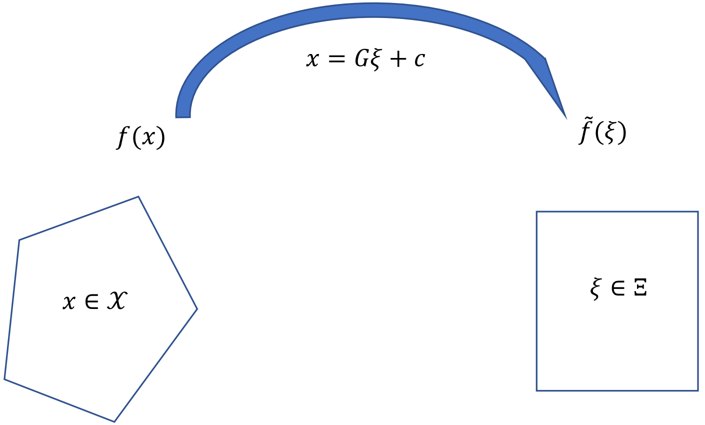




$$\mathcal{Z} = \{\tilde{G}\xi + \tilde{c} | \xi \in \mathbb{B}^{n_g}, \tilde{A}\xi = \tilde{b}\}$$

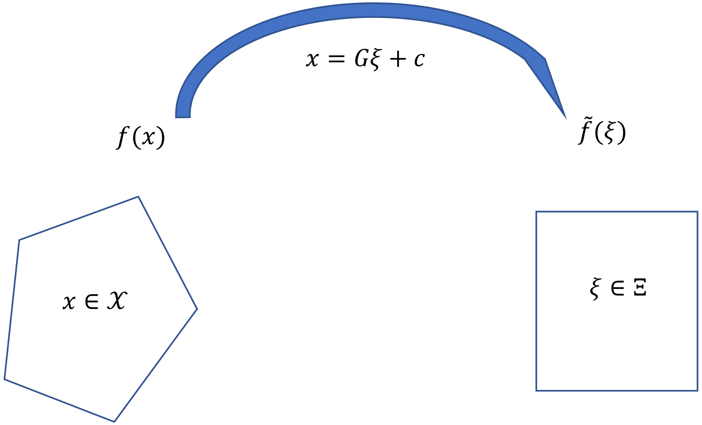
$$\mathcal{Z} = \bigcap_{s=1}^{S} \{G_s\zeta + c_s | \zeta \in \mathbb{B}^{\hat{n}_g}\}$$

Main Idea



- Now apply mixed-monotone decompositions in the space of generators (Ξ) for propagation and update

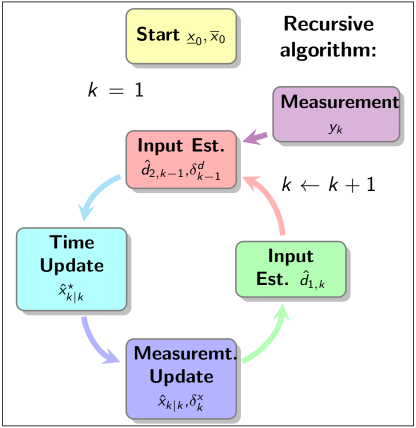
Main Idea



- Now apply mixed-monotone decompositions in the space of generators (Ξ) for propagation and update

Simultaneous State and Input Observer Design

- Design stable and optimal hyperball-valued observer

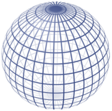


System with Unknown Inputs

$$x_{k+1} = f(x_k) + Bu_k + Gd_k + Ww_k,$$
$$y_k = Cx_k + Du_k + Hd_k + v_k,$$

- Find centers $\hat{x}_k, \hat{d}_{k-1}$ and radii $\delta^x_k, \delta^d_{k-1}$, such that:

$$\begin{cases} \|x_k - \hat{x}_k\|_2 \leq \delta^x_k \\ \|d_{k-1} - \hat{d}_{k-1}\|_2 \leq \delta^d_{k-1} \end{cases}$$



Residual-Based Mode Elimination

Theorem 10 (Mode Elimination Criterion)

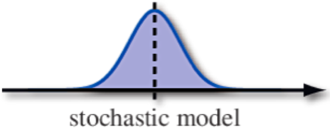
- $r_k^q \triangleq z_{2,k}^q - C_2^q \hat{x}_{k|k}^{\star,q} - D_2^q u_k^q$ *(residual signal)*
- $r_k^{q|*}$: *the true mode's residual signal (i.e., $q = q^*$)*
- $\delta_{r,k}^{q,*}$: *some tractable upper bound for the residual's norm, i.e.,* $\|r_k^{q|*}\|_2 \leq \delta_{r,k}^{q,*}$
- *Then, mode q is NOT the true mode, i.e., can be eliminated at time k, if $\|r_k^q\|_2 > \delta_{r,k}^{q,*}$.*

Residual-Based Mode Elimination

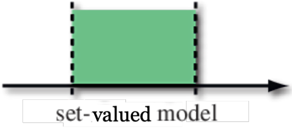
Theorem 10 (Mode Elimination Criterion)

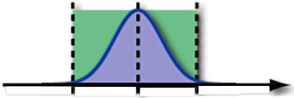
- $r_k^q \triangleq z_{2,k}^q - C_2^q \hat{x}_{k|k}^{\star,q} - D_2^q u_k^q$ *(residual signal)*
- $r_k^{q|*}$: *the true mode's residual signal (i.e., $q = q^*$)*
- $\delta_{r,k}^{q,*}$: *some tractable upper bound for the residual's norm, i.e.,* $\|r_k^{q|*}\|_2 \leq \delta_{r,k}^{q,*}$
- *Then, mode q is NOT the true mode, i.e., can be eliminated at time k, if* $\|r_k^q\|_2 > \delta_{r,k}^{q,*}$.

- How about considering different "uncertainty models"?



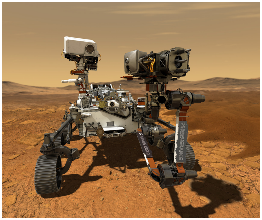
+



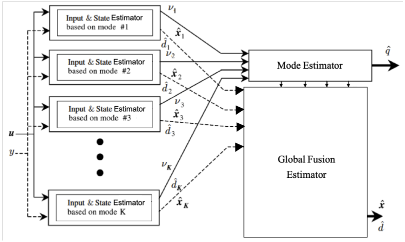


Truncated Gaussian Uncertainty (aleatoric+epistemic)

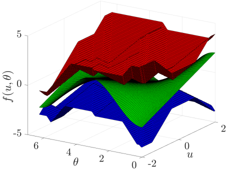
Future Vision: 4. Uncertain and Hybrid Networked CPS



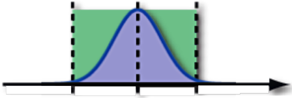
Hybrid reachability and invariance properties



Hidden mode CPS: MM framework



Unknown CPS: set-membership learning meets model-based approaches



Aleatoric+epistemic uncertainties: random sets

Mixed-Monotonicity; Further Interesting Implications

- reachability of nonsmooth & discontinuous systems
- computing controlled invariant sets
- reach-avoid-stay sets

Robust, Resilient, Safe & Private Autonomy

smart grid attack US

All | News | Images | Videos | Shopping | More

About 28,000,000 results (0.37 seconds)

https://www.wired.com › Security › security roundup

Attackers Keep Targeting the US Electric Grid - WIRED

Dec 10, 2022 — We at WIRED have written plenty about the threat that cyberattacks pose to power **grids** worldwide. But lately, the most significant **attacks** ...

https://www.gao.gov › blog › securing-u.s.-electricity-g...

Securing the U.S. Electricity Grid from Cyberattacks | U.S. GAO

Oct 12, 2022 — But the electricity **grid** is an attractive target for cyberattacks from **U.S.** ... **grid** vulnerable and what could happen if it were **attacked**?

Missing: ~~smart~~ | Must include: smart

https://www.theguardian.com › us-news › dec › us-pow...

Attacks on Pacific north-west power stations raise fears for US ...

Dec 10, 2022 — It's unknown who is behind the **attacks** but experts have long warned of discussion among extremists of disrupting the nation's power **grid**.

https://www.eenews.net › Articles

Attacks on grid infrastructure in 4 states raise alarm - E&E News

Dec 9, 2022 — Shootings at two electric substations in North Carolina last weekend are among the numerous threats posed to **U.S.** electric infrastructure ...

https://www.utilitydive.com › news › sophisticated-hack...

Sophisticated hackers could crash the US power grid, but ...

Oct 28, 2021 — Sophisticated hackers could crash the **US** power **grid**, but money, not sabotage, is their focus. For now, the capability remains in the hands ...

malicious drones in us

All | News | Images | Videos | Shopping | More

About 1,100,000 results (0.42 seconds)

https://thelastmile.gotennapro.com › Articles

Malicious drones – the UAS threat facing law enforcement and ...

Sep 8, 2022 — Unmanned ariel vehicles (UAVs) – which are more commonly referred to as "**drones**" – are practically everywhere today.

https://www.hstoday.us › Featured

Assessing the Risk to Soft Targets from Malicious Drones

Sep 4, 2022 — **Drone** threats to soft targets vary broadly. **Drones** may be used as reconnaissance for non-**drone** attacks, as the Christchurch shooter did. **Drones** ...

https://www.cisa.gov › unmanned-aircraft-systems

Unmanned Aircraft Systems (UAS) - Critical Infrastructure - CISA

However, UAS can also be used for **malicious** schemes by terrorists, ... systems (UAS)—also known as unmanned aerial vehicles (**UAV**) or **drones**—are used across ...

https://www.voanews.com › counter-drone-technology-...

Counter-drone Technology Stopping Malicious Drones from ...

Sep 27, 2022 — VOA's Julie Taboh reports on a company that has developed counter-**drone** technology that can identify and mitigate threats from **malicious** ...

https://www.voanews.com › logon-counter-drone-techn...

LogOn Counter-Drone Technology Prevents Malicious Drones ...

Nov 15, 2022 — VOA's Julie Taboh reports on a company that has developed counter-**drone** technology that can identify and mitigate threats from **malicious** ...

Design Strategy: JSS decomposition of vector fields

$$\left.\begin{aligned} x^+ &= f(x,w) = Ax + Bw + \underbrace{\phi(x,w)}_{\text{JSS}} \\ y &= h(x,v) = Cx + Dv + \underbrace{\psi(x,v)}_{\text{JSS}} \\ 0 &= L(y - Cx - Dv - \psi(x,v)) \end{aligned}\right\} \Longrightarrow$$

$$x^+ = \underbrace{(A - LC)x + Bw - LDv}_{f_\ell(\underbrace{x,w,v}_{\xi})} + Ly + \underbrace{\phi(x,w) - L\psi(x,v)}_{f_\nu(\underbrace{x,w,v}_{\xi})}$$

Linear + Nonlinear Embedding Systems

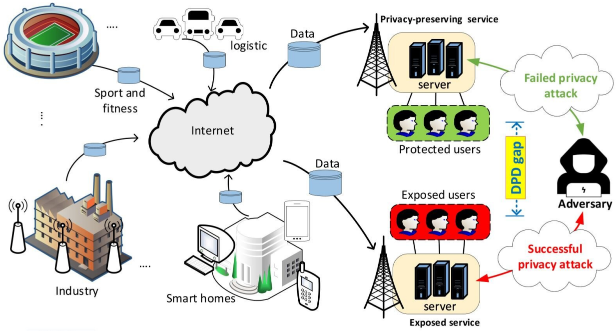
$$\begin{cases} \underline{x}^+ = f_{\ell d}(\underline{\xi},\overline{\xi}) + f_{\nu d}(\underline{\xi},\overline{\xi}) = (A-LC)^{\uparrow}\underline{x} - (A-LC)^{\downarrow}\overline{x} + Ly + \phi_d(\underline{x},\underline{w},\overline{x},\overline{w}) \\ \qquad -L^{\oplus}\psi_d(\overline{x},\overline{v},\underline{x},\underline{v}) + L^{\ominus}\psi_d(\underline{x},\underline{v},\overline{x},\overline{v}), \\ \overline{x}^+ = f_{\ell d}(\overline{\xi},\underline{\xi}) + f_{\nu d}(\overline{\xi},\underline{\xi}) = (A-LC)^{\uparrow}\overline{x} - (A-LC)^{\downarrow}\underline{x} + Ly + \phi_d(\overline{x},\overline{w},\underline{x},\underline{w}) \\ \qquad -L^{\oplus}\psi_d(\underline{x},\underline{v},\overline{x},\underline{v}) + L^{\ominus}\psi_d(\overline{x},\overline{v},\underline{x},\underline{v}) \end{cases}$$

Khajenejad, M. and Yong, S.Z. "$\mathcal{H}_\infty$-Optimal Interval Observer Synthesis for Uncertain Nonlinear Dynamical Systems via Mixed-Monotone Decompositions." *IEEE Control Systems Letters (L-CSS)*, pages 3008–3013, vol. 6, 2022 (presented in CDC'22).

Khajenejad, M., Shoaib, F. and Yong, S.Z. "Interval Observer Synthesis for Locally Lipschitz Nonlinear Dynamical Systems via Mixed-Monotone Decompositions." *American Control Conference (ACC)*, Atlanta, Georgia, pp. 2970–2975, 2022 (average acceptance rate: %67).

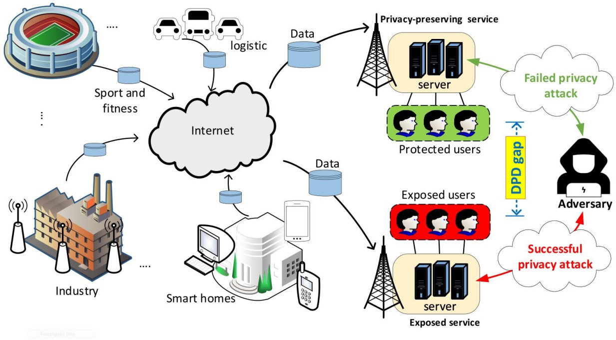
Pati T., **Khajenejad, M.**, Daddala S.P. and Yong, S.Z. "L_1-Robust Interval Observer Design for Uncertain Nonlinear Dynamical Systems." *IEEE Control Systems Letters (L-CSS)*, pages 3475–3480, vol. 6, 2022 (presented in CDC'22).

Future Vision: 3. Guaranteed Privacy-Preserving Mechanism Design



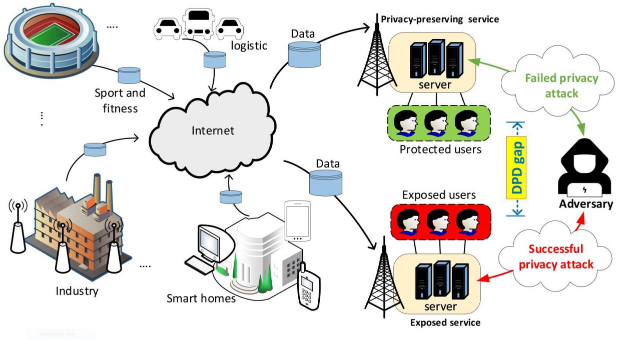
- Existing notions of privacy: either sacrifice accuracy or incur large computation or communication overhead
- Need for hard accuracy bounds
- Towards guaranteed private estimation, control and verification by leveraging unknown but deterministic functional perturbations

Future Vision: 3. Guaranteed Privacy-Preserving Mechanism Design



- Existing notions of privacy: either sacrifice accuracy or incur large computation or communication overhead
- Need for hard accuracy bounds
- Towards guaranteed private estimation, control and verification by leveraging unknown but deterministic functional perturbations

Future Vision: 3. Guaranteed Privacy-Preserving Mechanism Design



- Existing notions of privacy: either sacrifice accuracy or incur large computation or communication overhead
- Need for hard accuracy bounds
- Towards guaranteed private estimation, control and verification by leveraging unknown but deterministic functional perturbations