Dynamic Analysis of Cyber-Physical Systems

Parasara Sridhar Duggirala,
Sayan Mitra,
Mahesh Viswanathan

ILLINOIS

Motivation

- Cyber-Physical Systems : Systems that interact with physical environment and are controlled by a computer
- Distributed, nonlinear behavior

- Involves interaction between physical space and digital space
- Dynamic Analysis

Motivation

- Static analysis techniques: Reachability
  - Curse of Dimensionality
  - Techniques for analyzing networked systems are still preliminary

- Sample executions (test runs) are readily available

- Can we infer properties from sample executions?

Organization

- For continuous systems
  - Annotation assisted dynamic analysis
  - Notion of annotations
  - Dynamic analysis using annotations

- For networked systems
  - Distributed execution trace
  - Timing analysis
  - Inferring global properties

Part 1

Continuous Systems

Dynamic Analysis of Continuous Systems using Annotations

- *Annotations in software*
- Annotations for continuous variables
- Continuous behavior $\dot{x} = f_i(x,t)$, $x \in \mathbb{R}^n, t \in \mathbb{R}^{\geq 0}, I, \{f_i\}_{i \in I}$, $\Theta \subseteq \mathbb{R}^n$

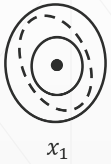
Dynamic Analysis of Continuous Systems using Annotations

- *Annotations in software*
- Annotations for continuous variables
- Continuous behavior $\dot{x} = f_i(x,t)$, $x \in \mathbb{R}^n, t \in \mathbb{R}^{\geq 0}$, $I, \{f_i\}_{i \in I}$, $\Theta \subseteq \mathbb{R}^n$
- Solution or trajectory for each mode i
  - ξ_i: $\mathbb{R}^n \times \mathbb{R}^{\geq 0} \to \mathbb{R}^n$
  - $\xi_i(\mathrm{x}_0, \mathrm{t})$: state of the system from $x_0 \in \Theta$ after time t

- Annotation would involve states and trajectories

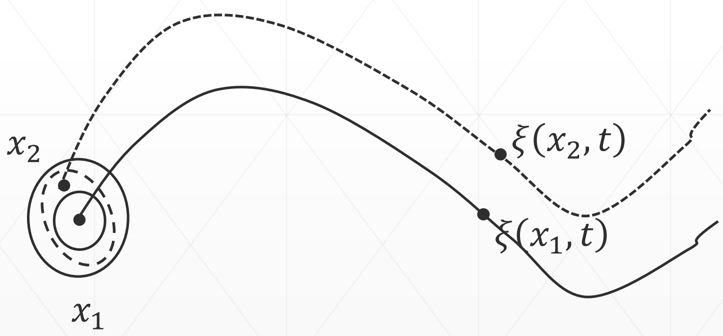
Annotations: Discrepancy function

- Definition. A smooth function $V : \mathbb{R}^{2n} \rightarrow \mathbb{R}^{\geq 0}$ is a *discrepancy function* for $\dot{x} = f(x, t)$ if for any x_1 and $x_2 \in \mathbb{R}^n$
    1. (static bound) $\exists\ \alpha_1, \alpha_2\text{:}\ \alpha_1(|x_1 - x_2|) \leq V(x_1, x_2) \leq \alpha_2(|x_1 - x_2|)$
    2. (dynamic bound) $V(\xi(x_1, t), \xi(x_2, t)) \leq \beta(x_1, x_2, t)$ where $\beta\text{:}\ \mathbb{R}^{2n} \times \mathbb{R}^{\geq 0} \rightarrow \mathbb{R}^{\geq 0}$ and $\beta \rightarrow 0$ as $x_1 \rightarrow x_2$



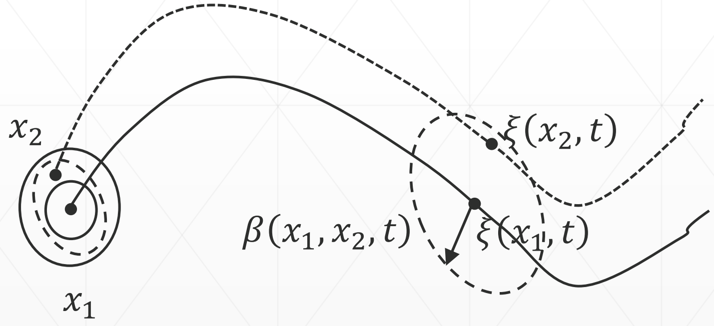
Annotations: Discrepancy function

- Definition. A smooth function $V : \mathbb{R}^{2n} \to \mathbb{R}^{\geq 0}$ is a *discrepancy function* for $\dot{x} = f(x,t)$ if for any x_1 and $x_2 \in \mathbb{R}^n$
    1. (static bound) $\exists\ \alpha_1, \alpha_2$: $\alpha_1(|x_1 - x_2|) \leq V(x_1, x_2) \leq \alpha_2(|x_1 - x_2|)$
    2. (dynamic bound) $V(\xi(x_1,t), \xi(x_2,t)) \leq \beta(x_1, x_2, t)$ where $\beta: \mathbb{R}^{2n} \times \mathbb{R}^{\geq 0} \to \mathbb{R}^{\geq 0}$ and $\beta \to 0$ as $x_1 \to x_2$



Annotations: Discrepancy function

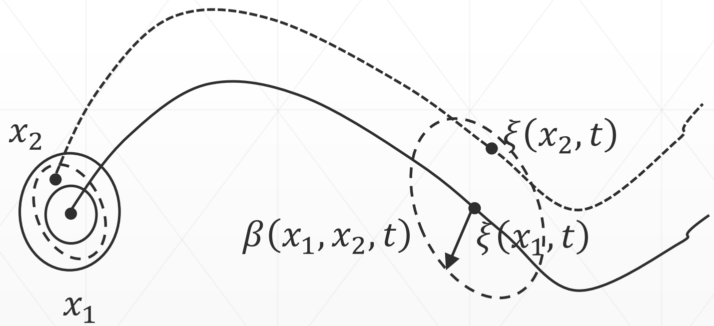
- Definition. A smooth function $V : \mathbb{R}^{2n} \rightarrow \mathbb{R}^{\geq 0}$ is a *discrepancy function* for $\dot{x} = f(x,t)$ if for any x_1 and $x_2 \in \mathbb{R}^n$
  1. (static bound) $\exists\ \alpha_1, \alpha_2$: $\alpha_1(|x_1 - x_2|) \leq V(x_1, x_2) \leq \alpha_2(|x_1 - x_2|)$
  2. (dynamic bound) $V(\xi(x_1,t), \xi(x_2,t)) \leq \beta(x_1, x_2, t)$ where $\beta: \mathbb{R}^{2n} \times \mathbb{R}^{\geq 0} \rightarrow \mathbb{R}^{\geq 0}$ and $\beta \rightarrow 0$ as $x_1 \rightarrow x_2$



Annotations: Discrepancy function

- Definition. A smooth function $V : \mathbb{R}^{2n} \rightarrow \mathbb{R}^{\geq 0}$ is a *discrepancy function* for $\dot{x} = f(x,t)$ if for any x_1 and $x_2 \in \mathbb{R}^n$
  1. (static bound) $\exists\, \alpha_1, \alpha_2 \colon \alpha_1(|x_1 - x_2|) \leq V(x_1, x_2) \leq \alpha_2(|x_1 - x_2|)$
  2. (dynamic bound) $V(\xi(x_1,t), \xi(x_2,t)) \leq \beta(x_1, x_2, t)$ where $\beta \colon \mathbb{R}^{2n} \times \mathbb{R}^{\geq 0} \rightarrow \mathbb{R}^{\geq 0}$ and $\beta \rightarrow 0$ as $x_1 \rightarrow x_2$

- $(\alpha_1, \alpha_2, \beta)$ is a witness for V



- Stability not required
- Multiple annotations for the same system

About Annotations

- Comparing different annotations:
  - Lipschitz Constant : Exponential divergence
  - Contraction Metric : Exponential Convergence
  - Incremental Stability : Convergence
  - Extension of Incremental Stability called Incremental Forward Completeness

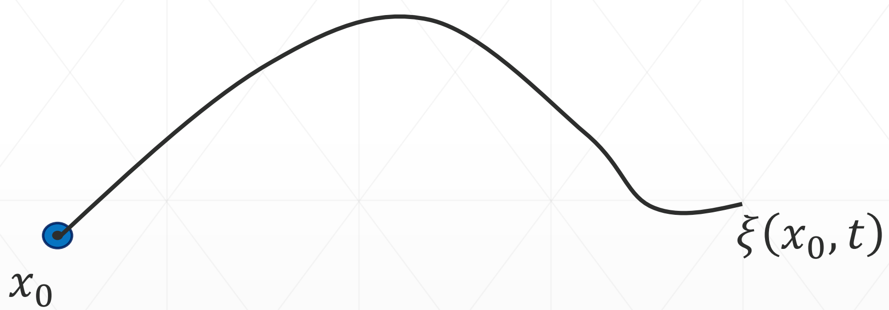
- Discrepancy function does not require convergence

About Annotations

- How are annotations useful : computing sound over approximations

$$\forall\, x \in B_\delta(x_0), \xi(x,T) \in B_\varepsilon^V\big(\xi(x_0,T)\big)\ where\ \varepsilon = \sup_{x\, \in B_\delta(x_0), 0 \le t \le T} \{\beta(x, x_0, t)\}$$

$$B_\varepsilon^V(x) = \{\, x' \,|\, V(x, x') \le \ \varepsilon\}$$

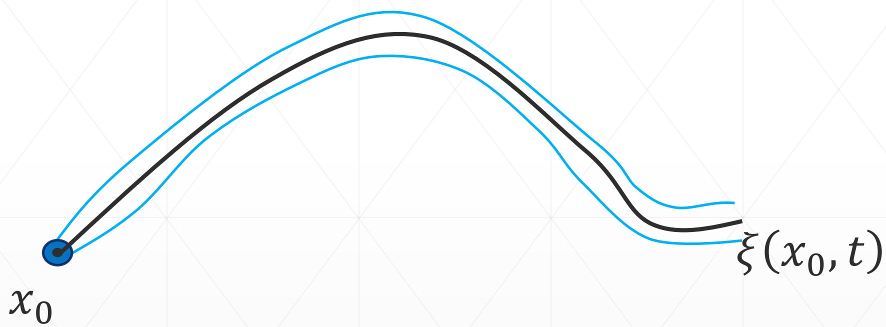


About Annotations

- How are annotations useful : computing sound over approximations

$$\forall\, x \in B_\delta(x_0), \xi(x,T) \in B_\varepsilon^V\big(\xi(x_0,T)\big)\ where\ \varepsilon = \sup_{x\, \in B_\delta(x_0), 0\le t\le T} \{\beta(x,x_0,t)\}$$

$$B_\varepsilon^V(x) = \{\, x' \,|\, V(x,x') \le\ \varepsilon\}$$

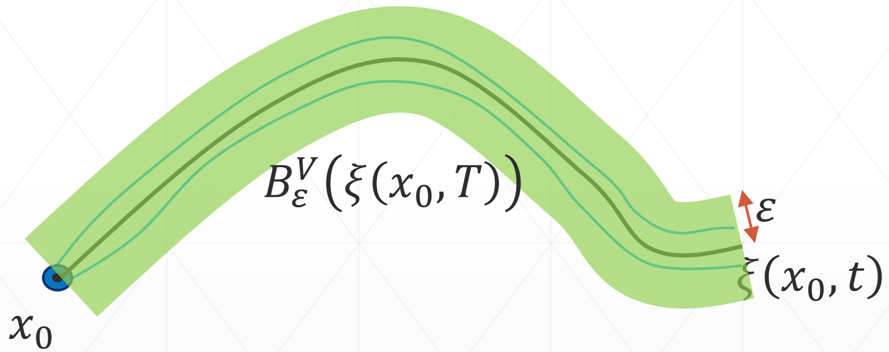


About Annotations

- How are annotations useful : computing sound over approximations

$$\forall\, x \in B_\delta(x_0), \xi(x,T) \in\; B_\varepsilon^V\big(\xi(x_0,T)\big)\; where\ \varepsilon = \sup_{x\, \in B_\delta(x_0), 0\le t\le T} \{\beta(x, x_0, t)\}$$

$$B_\varepsilon^V(x) = \{\, x' \,|\, V(x,x') \le\; \varepsilon\}$$



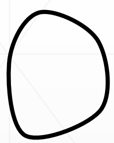
Basic Algorithm

- Partition, Simulate, Bloat, Check

Unsafe set

$$\dot{x} = f_i(x, t)$$

$$\xi_i\colon \mathbb{R}^n \times \mathbb{R}^{\geq 0} \rightarrow \mathbb{R}^n$$

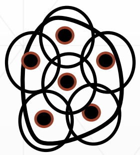


Initial Set

Basic Algorithm

- Partition, Simulate, Bloat, Check

$$\dot{x} = f_i(x, t)$$
$$\xi_i\colon \mathbb{R}^n \times \mathbb{R}^{\geq 0} \to \mathbb{R}^n$$

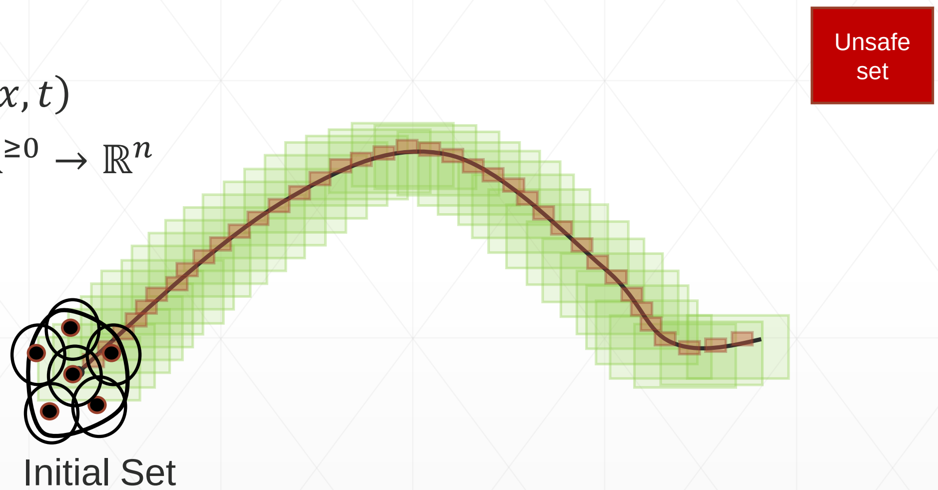


Basic Algorithm

- Partition, Simulate, Bloat, Check, Refine

$$\dot{x} = f_i(x, t)$$

$$\xi_i \colon \mathbb{R}^n \times \mathbb{R}^{\geq 0} \rightarrow \mathbb{R}^n$$

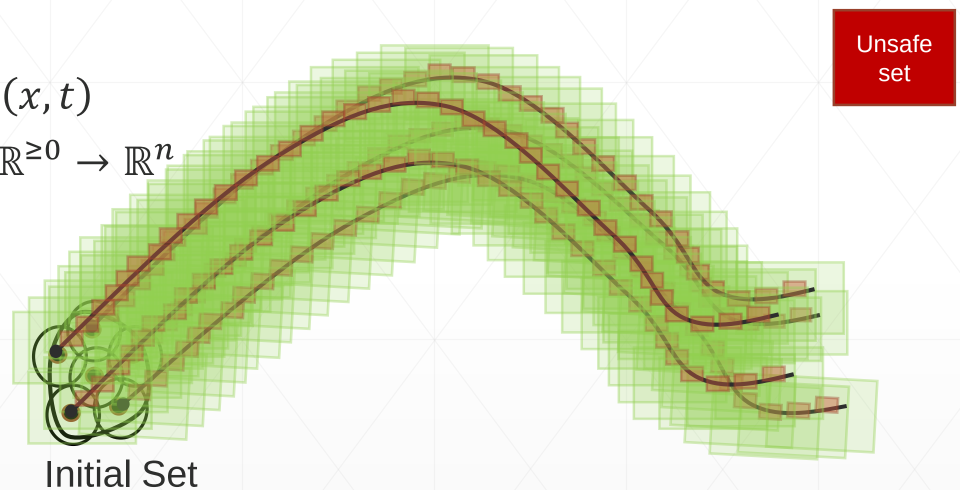


Basic Algorithm

- Partition, Simulate, Bloat, Check, Refine

$$\dot{x} = f_i(x, t)$$

$$\xi_i \colon \mathbb{R}^n \times \mathbb{R}^{\geq 0} \rightarrow \mathbb{R}^n$$



- If Unsafe set is reachable, then we refine the initial partitioning

Guarantees

- Soundness: If the algorithm infers that the system is safe (unsafe), then the system is indeed safe (unsafe).
- Relative Completeness: If the system is robustly safe (unsafe), then the algorithm terminates and returns that that the system is safe (unsafe).

Experimental Results

Benchmark	Variables	Time horizon	Refs.	Sims.	C2E2 (sec)	Flow* (sec)	Ariadne (sec)
Moore-G. Jet Engine	2	10	12	36	1.56	10.54	56.57
Brussellator	2	10	33	115	5.26	16.77	72.75
VanDerPol	2	10	5	17	0.75	8.93	98.36
Coupled VanDerPol	4	10	10	62	1.43	90.96	270.61
Sinusoidal Tracking	6	10	12	84	3.68	48.63	763.32
Linear Adaptive	3	6	8	16	0.47	NA	NA
Nonlinear Adaptive	2	10	16	32	1.23	NA	NA
Nonlinear Disturbance	3	10	22	48	1.52	NA	NA

Benchmark	Sims.	Time (sec)
12 fluid tanks (ft)	16	2.74
18 ft	76	15.28
24 ft	100	22.12
30 ft	124	28.82
3 vehicles 12 vars	32	5.68
16 vars	64	12.23
20 vars	128	25.14
24 vars	256	54.23

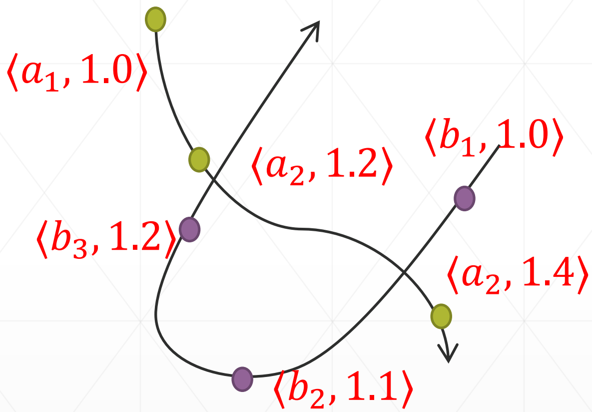
Switched-Nonlinear models

Part 2

Networked Systems

Challenges and Problem Statement

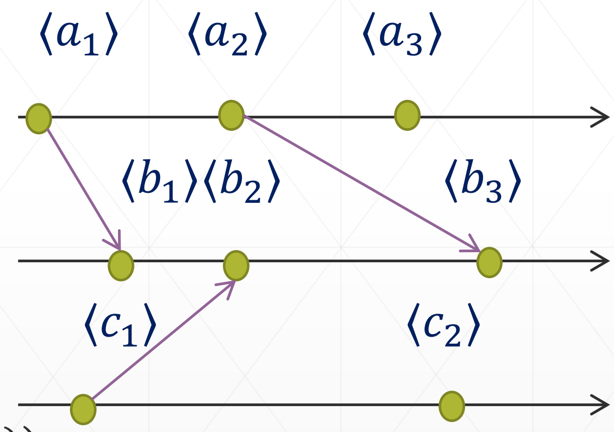
- **Nondeterminism**: concurrency, message losses, delays, clock drifts, scheduling, …
- Each agent generates time-stamped observations: $\rho_i = \langle x_{i1}, clk_{i1}\rangle \ldots \langle x_{ik}, clk_{ik}\rangle$
- Clocks imperfectly synchronized
- System trace ρ is a collection $\{\rho_i\}$
- Discrete & continuous evolution



Given ρ, a model or annotation A, and a global property U, is every ρ-consistent execution of A safe with respect to U?

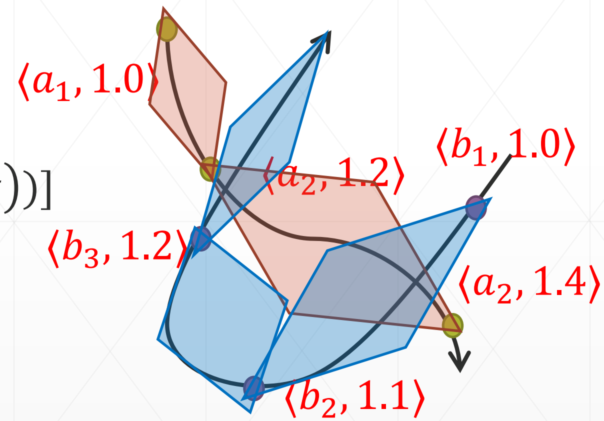
Real-time bounds from messages

- ρ is σ-synchronized if for every $\langle x_i, clk_i \rangle$ consistent execution ξ, there exists $t_i \in [clk_i - \sigma, clk_i + \sigma]$ when $\xi(x_0, t_i) = x_i$
- $L(x_i)$: Greatest lower bound on real-time for occurrence of x_i on all consistent executions
- $L(x_i) = max\left(clk_i - \sigma, \max_{y_j \leftarrow x_i} U(y_j)\right)$
- $\boldsymbol{y_j} \leftarrow \boldsymbol{x_i}$ in ρ if and only if
  1) $j = i$ and x_i is recorded after y_j or
  2) $y_j = send(m)$ and $x_i = receive(m)$
  3) $y_j \leftarrow w$ and $w \leftarrow \boldsymbol{x_i}$
- $U(x_i)$: *Least upper bound* = $min\left(clk_i + \sigma, \max_{x_i \leftarrow y_j} L(y_j)\right)$
- For observation $\langle x_i, clk_i \rangle$ we have (*tight*) *observation intervals* $[L(x_i), U(x_i)]$



Symbolic Over-approximation

- $\mathbf{A}$: hybrid model
- $Post(\mathbf{A}, x_j, t)$: Reach from x_j in t time
- $Pre(\mathbf{A}, x_j, t)$: Reach to x_j in t time
- $Reach(A, \{x_1, \ldots, x_m\}, t)$: Reachable through $\rho = x_1, \ldots, x_m$ at t
- $Reach(A, \{x_1, \ldots, x_m\}, t) = \exists t_1 < \cdots < t_m$:
  - $\wedge_{j=1}^{m} \ L(x_j) \leq t_j \leq U(x_j)$
  - $\wedge_{j=1}^{m-1} t_j \leq t \leq t_{j+1} \Rightarrow \ (Post(x_j, t - t_j) \wedge Pre(x_{j+1}, t_{j+1} - t))]$
- Check $\forall t \ Reach(\rho, t) \Rightarrow \neg U$



Soundness

- Theorem. For any trace ρ,

  If for all t $Reach(\rho, t) \Rightarrow \neg U$

  then all executions consistent with ρ are safe

  with respect to U.

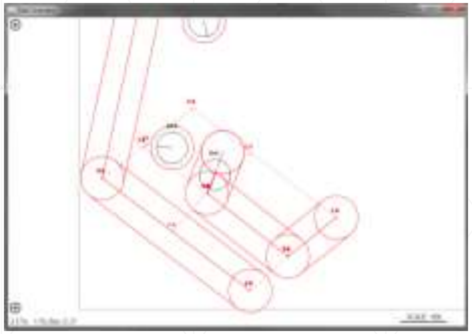
Relative Completeness

- A trace ρ is tightly σ-synchronized with respect to model A if in addition to being σ-synchronized, for every t $\in [clk_i - \sigma, clk_i + \sigma]$ there is a consistent execution ξ with $\xi(x_0, t) = x_i$.

- Theorem. If Post*() & Pre() are* exact and ρ is tightly σ-synchronized, then every state in $Reach(\beta, t)$ is visited by some ρ-consistent execution at time t.

Experiments: Debugging robot apps!

- Applications & properties
  - Waypoint following with obstacle avoidance
  - GeoCast: For geocast(m,R) at time t
    - Every robot within R during [t+a,t+b] receives m
    - No robot outside R during [t+a',t+b'] receives m
  - Light painting: Create pictures on the floor without collisions and deadlocks



Experiments: Scaling and Precision

N	x = 75 ms	150 ms	250 ms	500 ms
4	42	24	10	5
8	92	48	22	10
12	246	114	34	16
16	10 m	4 m	49	24
20	20 m	8 m	67	34

Always separation (d = 10 cm) for 5 mins @ x ms

	VB = ± 0 cm/s	VB = ± 20 cm/s	VB = ± 20 cm/s
	Separation (d=10 cm)		
OI = $\pm 5ms$	yes	yes	no
OI = $\pm 10ms$	yes	no	no
OI = $\pm 20ms$	no	no	no
	Georeceive		
delay = 0ms	yes	yes	yes
delay = 20ms	yes	yes	no
delay = 50ms	no	no	no

System model **precision**

VB: velocity bounds, OI: observation intervals

Lower precision model ($\pm 20ms$) produces **more conservative** than the higher precision models ($\pm 5ms$)

Conclusions

- Dynamic analysis for hybrid systems using annotations
- Symbolic overapproximation for distributed cyber-physical systems
- Infer global predicates with soundness and completeness guarantees

References

- *Parasara Sridhar Duggirala, Sayan Mitra, Mahesh Viswanathan,* “**Verification of Annotated Models from Executions**”, International Conference on Embedded Software (EMSOFT) 2013

- *Parasara Sridhar Duggirala, Taylor Johnson, Adam Zimmerman, Sayan Mitra,* “**Static and Dynamic Analysis of Timed Distributed Traces**”, IEEE Real-Time Systems Symposium (RTSS) 2012