# CAREER: Robust Verification of Cyber Physical Systems (CPS)

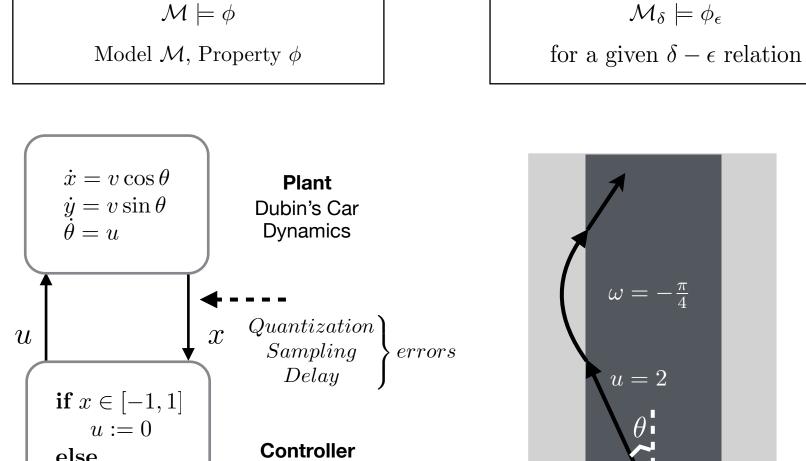
#### PI: Pavithra Prabhakar

Associate Professor, Department of Computer Science, Kansas State University, Manhattan, KS (pprabhakar@ksu.edu)

### Robust verification

Guarantee system correctness even in the presence of perturbations.

**Robust Verification Problem** 



Control logic for

autonomous driving

**Classical Verification Problem** 

 $u := \omega$ 

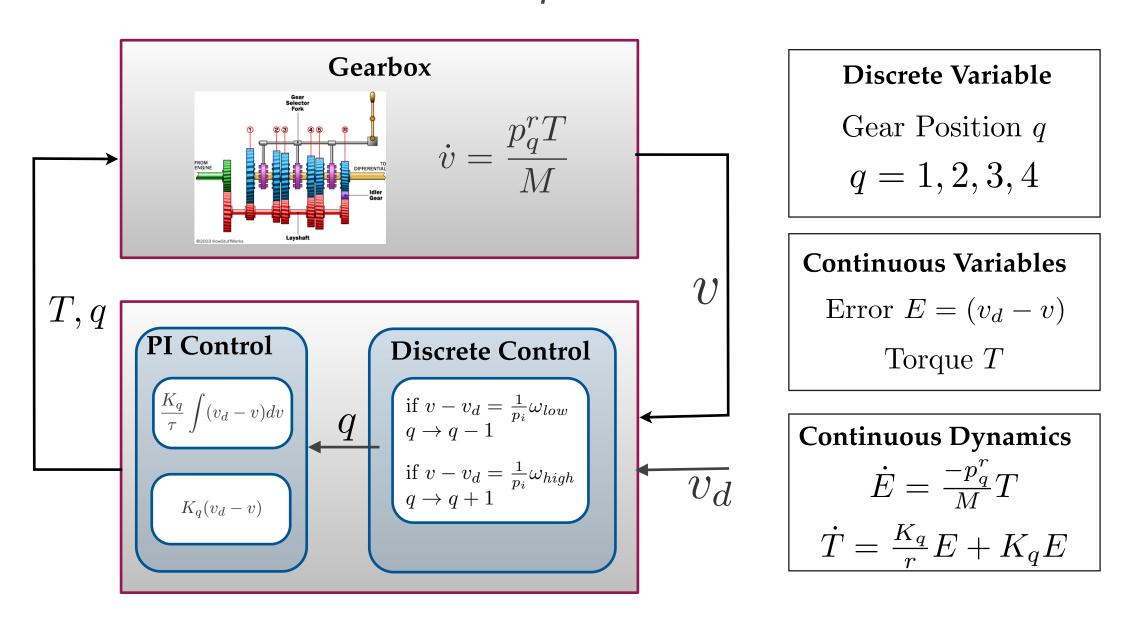
Autonomous vehicle controller

**Challenges:** Classical analysis techniques do not extend in a straight forward manner to the robust verification problem owing to its quantitative/ topological aspects.

Goal in autonomous driving: Keep the vehicle on the road even in the presence of perturbations due to quantization of sensor data, sampling and sensing, actuation or communication delays.

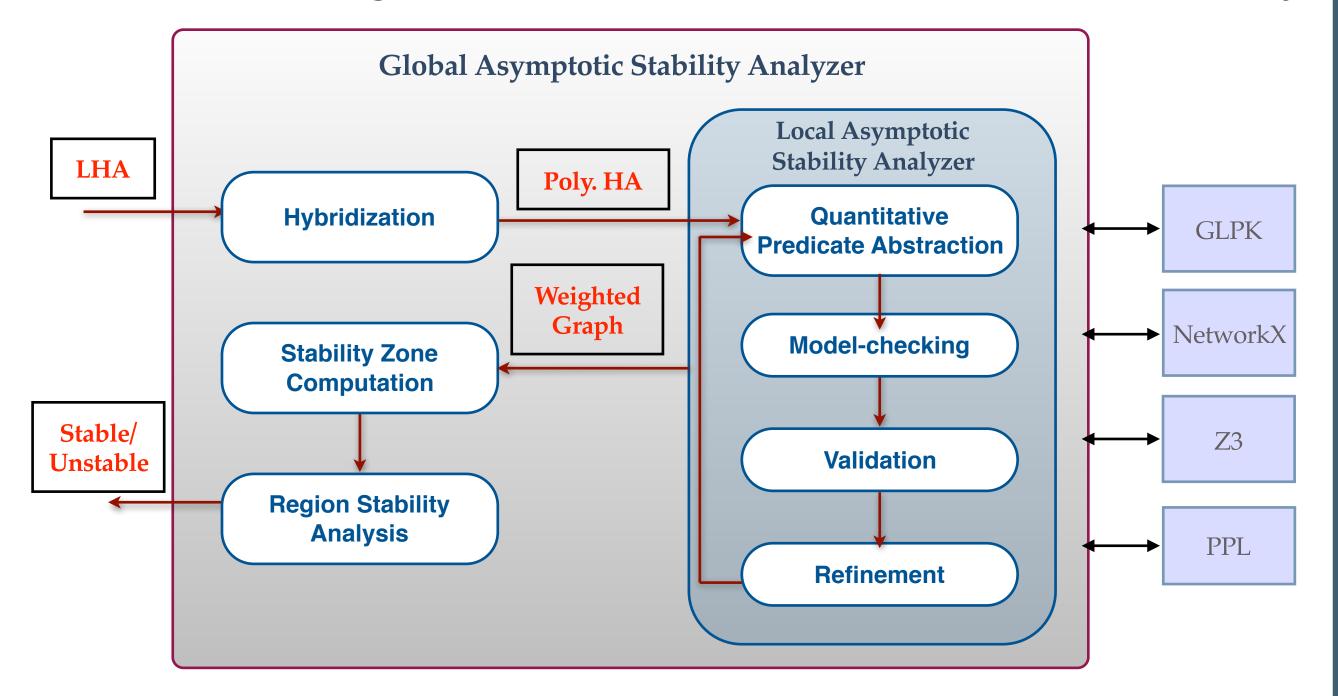
### Stability in Cruise Control

Small perturbations in the initial state/input lead to small deviations in behavior.



Automatic Gearbox & Cruise Control: Maintain the velocity of the vehicle at the desired velocity.

# AVERIST: Algorithmic Verifier for Stability

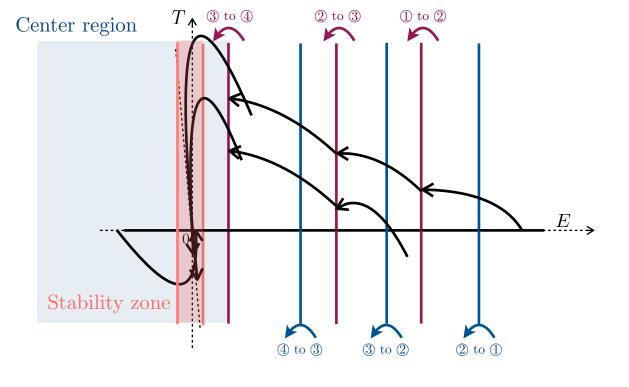


Tool webpage: <a href="http://software.imdea.org/projects/averist/">http://software.imdea.org/projects/averist/</a>

### Analysis

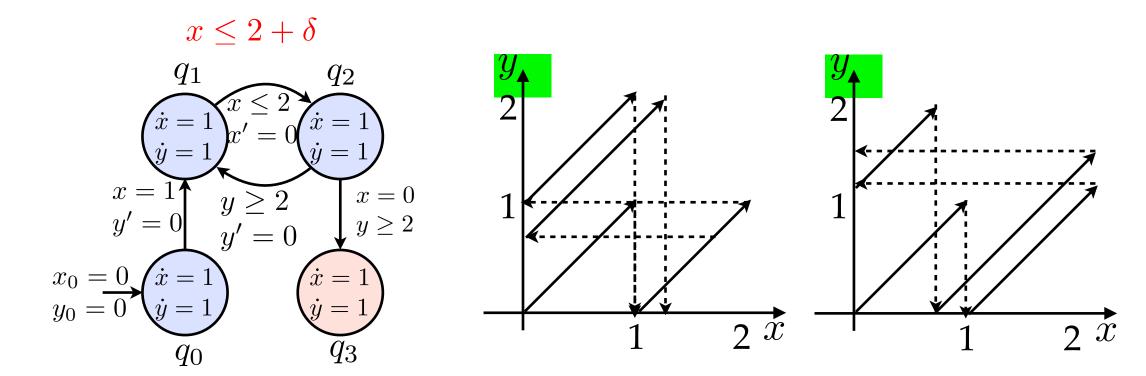
		AVERIST			STABHYLI		
Dimension/ name		Regions	Runtime	Proved Stability	Degree	LF found	Runtime
2D	AS1	129	31	Yes	6	Yes	8
	SS4 1	9	<1	Yes	8	-	452
	SS8 1	17	<1	Yes	6	-	443
	SS16 1	33	1	Yes	4	-	177
3D	AS 4	147	194	Yes	6	_	410
	SS4 4	771	484	Yes	2	Yes	75
	SS8 4	771	470	Yes	2	Yes	15
	SS16 4	771	568	Yes	2	Yes	138
4D	AS 7	81	625	Yes	2	-	12
	SS4 7	81	119	Yes	2	-	101
	SS8 7	153	234	Yes	2	_	1071
	SS16 7	297	533	Yes	2	-	339
	AS 9	_	out	No	4	Yes	34
	SS4 9	81	125	Yes	4	_	105
	SS8 9	153	247	Yes	2	_	16

- 1. Linear to polyhedral dynamics abstraction.
- 2. QPA to prove local asymptotic stability.
- 3. Stability zone construction using QPA.
- 4. Region stability with respect to stability zone.



- Averist proves stability in many more cases than Stabhyli.
- AVERIST is more numerically stable.
- \* AVERIST is easily amenable to parallelization.

### Clock Drifts & Guard Perturbations



#### **Observations:**

- Small syntactic perturbations can lead to large semantic perturbations.
- The timed automaton is safe (does not reach the green region), but any small perturbation of its guards violates safety.

#### **Problems:**

- Are there restrictions under which small syntactic perturbations lead to small semantic deviation?
- Can we decide if there is a small syntactic perturbation under which the systems satisfies a given property?

## Decidability of Robust Verification

**Omega Regular Property verification for timed automata:** 

Does every execution of the system reach a final state infinitely often?  $\mathcal{M} \models \Box \Diamond F$ ?

Satisfaction with clock drifts and perturbed guards:  $\exists \epsilon > 0, \delta > 0, \mathcal{M}^{\epsilon}_{\delta} \models \Box \Diamond F$ ?

Theorem: A system satisfies an omega regular property for some positive clock drifts and guard perturbations if and only if it satisfies the omega regular property for some positive clock drifts.

$$\exists \epsilon > 0, \delta > 0, \mathcal{M}_{\delta}^{\epsilon} \models \Box \Diamond F \Leftrightarrow \exists \delta' > 0, \mathcal{M}_{\delta'} \models \Box \Diamond F$$

The robust model-checking problem with only perturbations to the guards is shown to be decidable by Bouyer et al.

Corollary: The robust ω-regular model checking problem when both guards and clocks are perturbed is PSPACE-complete.

Theorem: Reachable sets under infinitesimal clock perturbations can be computed in space polynomial in the size of the timed automata.

### Syntactic vs Semantic Perturbations

 $Dist(\mathcal{M}_1, \mathcal{M}_2)$ : smallest  $\epsilon$  such that  $\mathcal{M}_1 \prec_{\epsilon,k} \mathcal{M}_2$  ( $\epsilon$  simulation up to k steps)

**Theorem:** Given  $\mathcal{M}$  defined using bounded continuous functions, for every  $\epsilon > 0$  and bound k, there exists  $\delta > 0$  such that  $Dist_k(\mathcal{M}, \mathcal{M}_{\delta}) \leq \epsilon$ .

Key Technical Result: Every predicate can be arbitrarily over-approximated

 $\forall \epsilon > 0, \exists \delta > 0, \llbracket \varphi^{\delta} \rrbracket \subseteq B_{\epsilon}(\llbracket \varphi \rrbracket)$ 

 $Dist_k$  is a continuous operator on the space of hybrid automata **Broad idea:** 

#### Completeness of counter-example validation and Delta complete bounded verification problem:

 $\delta$ -Complete Decision Problem:

Input: System  $\mathcal{M}$ , bound k, perturbation  $\delta$  and unsafe set U

Output:  $Reach_k(\mathcal{M}) \cap U = \emptyset$  or  $Reach_k(\mathcal{M}_{\delta}) \cap U \neq \emptyset$ 

**Theorem:** Given  $\mathcal{M}$ , a bound k and an unsafe predicate U,  $Reach_k(\mathcal{M}) \cap U = \emptyset$ implies  $\exists \delta > 0, Reach_k(\mathcal{M}_{\delta}) \cap U = \emptyset.$ 

### Future Research

- \* Hybridization for stability analysis of non-linear hybrid automata, where non-linear dynamics is abstracted to linear inclusion dynamics.
- Compositional analysis of stability for hybrid systems.
- \* Formal synthesis of switching logic for stability objectives, including periodically switched systems.
- Stochastic hybrid systems verification where uncertainties are captured as stochastic elements.

#### **Research Outputs:**

- M. G. Soto, P. Prabhakar. Averist: Algorithmic Verifier for Stability of Linear Hybrid Systems. 21st Hybrid Systems: Computation and Control (HSCC), 2018.
- N. Roohi, P. Prabhakar, M. Viswanathan. Relating Syntactic and Semantic Perturbations of Hybrid Automata. 29th International Conference on Concurrency Theory (CONCUR), 2018.
- A. Kundu, M. G. Soto, P. Prabhakar. Formal Synthesis of Stabilizing Controllers for Periodically Controlled Linear Switched Systems. 5th Indian Control Conference (ICC), 2018.
- P. Prabhakar, M. G. Soto. Formal Synthesis of Stabilizing Controllers for Switched Systems. 20th Hybrid Systems: Computation and Control (HSCC), 2017.
- N. Roohi, P. Prabhakar, M. Viswanathan. Robust Model Checking of Timed Automata under Clock Drifts. 20th Hybrid Systems: Computation and Control (HSCC), 2017.