C2E2: Simulation-Based Verification of Hybrid Systems

Parasara Sridhar Duggirala, Chuchu Fan, Matthew Potok, Bolun Qi, Sayan Mitra, Mahesh Viswanathan
Outline

• CPS Verification – challenges
• C2E2 – simulation based verification technique for CPS verification
• Features of C2E2
• Demo
Safety verification problems in CPS

hybrid model, requirements → C2E2 → bug trace, certificate

[Image of a car, highway, and an X-ray]
Auto-passing system

The diagram illustrates the maneuver phases of an auto-passing system. The system switches between different phases based on the distance and velocity of the vehicles. The phases include:

1. **Switch to left**
2. **Overtake**
3. **Gain threshold dist. d**
4. **Switch to right**

The system adjusts its behavior based on the variables $s_x$, $v_x$, and $a_x$, which represent the position, velocity, and acceleration, respectively. The system also takes into account the threshold distance $d$ and the angular velocity $\omega$.
Safety verification problem of ODEs

Consider an nonlinear ODE model \( \dot{x} = f(x), x \in \mathbb{R}^n \)

Discrete transitions

Reach\((\Theta, T)\): states reachable from initial set \( \Theta \subseteq \mathbb{R}^n \) up to time \( T \)

Safety verification problem: given initial set \( \Theta \), unsafe set \( U \), time bound \( T \), decide whether \( \text{Reach}(\Theta, \infty) \cap U = \emptyset \)

Safety verification is undecidable in general [Henzinger et al., 95]

Bounded time verification with over-approximation in existing tools:
- Linear dynamics: PHAVer [Frehse 05], SpaceEx [Frehse 11], \( d/dt \) [Asarin 01],
- Nonlinear dynamics: Flow* [Chen 12], etc.

C2E2: bounded time verification for nonlinear hybrid systems
- Simulation-driven approach
- Provides soundness and relative completeness guarantees
Automatic simulation-driven strategy

• Given start $\Theta$ and unsafe $U$
• Compute finite cover of initial set
• Simulate from the center $x_0$ of each cover
• **Bloat** simulation so that bloated tube contains trajectories from the cover
• Union = over-approximation of reach set
• Check intersection/containment with $U$ and refine
Verification of auto-passing system
Auto-passing system – counter-example
New features in C2E2

**Usability improvement**
- Automatic reachability with piece-wise on-the-fly discrepancy algorithm

**Efficiency improvement**
- Automatic detection and handling of different classes dynamics
  - Global discrepancy function for linear dynamics $\dot{x} = Ax$
  - On-the-fly discrepancy for nonlinear dynamics $\dot{x} = f(x)$
  - Special handling of constant dynamics $\dot{x} = k$

**New testing scripts and a command line interface**
Demo

1. Website, downloading, and installation instructions.
2. C2E2 usability features.
3. Verification, results, and visualizations.
   • Cardiac cell
   • Autonomous vehicle passing
   • Powertrain control system
   • Robotic arms
4. Reachable sets, other data.
Conclusion

Simulation-driven verification can be used for safety analysis of CPS

Automatic reachability analysis
Provides soundness and relative completeness

C2E2: our invariant verification tool for hybrid systems is able to solve some hard problems--try it

Check out more examples at the C2E2 webpage
https://publish.illinois.edu/c2e2-tool/
Questions?

Send an email to psd@uconn.edu, cfan10@illinois.edu or c2e2help@gmail.com