Online Hybrid Automata Verification of Dynamical Cyber-Physical System

Lei Bu
Nanjing University
bulei@nju.edu.cn

Joint Work with Qixin Wang and Xuandong Li
September 20th, Clarke Symposium 2014
Congratulations to Ed!

I was a visiting student in Ed’s group Sep 07-Sep 08

Great Mentor, I learned a lot from here

E.g. Cyber-Physical System
Outline

- Motivation
- Offline Modeling and Verification?
- Online Modeling and Verification
- Conclusion
Outline

- Motivation
- Offline Modeling and Verification?
- Online Modeling and Verification
- Conclusion
Motivation

- Cyber-Physical System
- Safety-Critical Area
- Verification
Motivating Example 1

- Communication-Based Train Control System
- **Train Control System**
  - Train communicates with RBC for new MA by 500ms.
  - If a train touches a SBD point, brake normally.
  - If a train has not get any info for 5s, brake emergently!

- **Specification**
  - No Collision!
Motivating Example 2

- Medical Cyber Physical System

Diagram:
- Supervisor
- Surgeon
- O₂ Sensor
- SpO₂ Sensor
- Ventilator
- Laser Scalpel
- Patient
Safety Rule

- Safety Rule 1: when the laser scalpel emits laser, the patient’s trachea oxygen level must not exceed a threshold $\Theta_{O_2}$ Fire!
- Safety Rule 2: the patient’s blood oxygen level never reaches below a threshold $\Theta_{SpO_2}$ Suffocation!
Outline

- Motivation
- Offline Modeling and Verification?
- Online Modeling and Verification
- Conclusion
Train

Continuous Realtime Behavior

Hybrid Behavior

Discrete Logic Control
Hybrid Automata
- Discrete Logic Transition
- Continuous Real-Timed Behavior
- Most Natural Model for CPS System

Our Target
- Model the Target CPS Systems by HA
- Verify it by Model Checking
Modeling

Specification:
Location: Sbraking; Constraint: Traini.x>ma

Problem: Lots of Free Parameters Included in the control functions: Windspeed, train mass, raining, etc.
Blood oxygen level is strongly affected by complex human body biochemical reactions, even emotions. No way to model $SpO_2$ in a long run.
Outline

- Motivation
- Offline Modeling and Verification
- Online Modeling and Verification
- Conclusion
Online periodical real-time hybrid systems model checking of time-bounded (i.e., short-run) future!

Traditional model checking vs. Ours:

Offline ↔ Online Periodical Real-Time

Long-Run Future ↔ Short-Run Future

Challenge 1: No good offline long run models for nondeterministic parameters.

After the key parameters’ values are fixed, the system’s online short-run behavior is easy to predict.

Challenge 2: Verification state space easily explode.

Online → Fixes Many Parameters

Short-Run → Shrink State Space
System Control

Classical Control Loop

Running System

Instructions Received

Actuator/Sensor

Control Function

New Value of Parameter

New Parameter Deployed

Parametric Model

Concretized Model

Online Modeling Module

Predefined Verification Task

Online Verification Module

Verification Rejected
Ask the System to call fall-back plan

Runtime Monitor
Performance Issue

- Periodically online verification -> **Have to Be Fast!**

- The model updates every T time unit, if we cannot finish the online modeling and verification in D time unit, the result will be useless
- Multicore Assignment Distribution
- Incremental Online Verification
- Our Own Tool BACH\textsubscript{OL}…
Evaluation

Train Control System
10 train 109ms < 500ms
(The first number is the mean value, the second number is the updating period)

Laser Scalpel
932ms < 4 s

ICCPS 11 WIP, ICCPS 12, DSN 13, TPDS
Motivation

Offline Modeling and Verification

Online Modeling and Verification

Conclusion
Conclusion

- Offline M&V $\Rightarrow$ Online M&V
- Non-deterministic $\Rightarrow$ Periodically deterministic
- Fast Verification
- Ongoing Work
  - Pipeline Design Based State Space Coverage
Thanks

Q&A