Toward Online Hybrid Systems Model Checking of Cyber-Physical Systems Time-Bounded Short-Run Behavior

Lei Bu*, Qixin Wang†, Xin Chen*, Linzhang Wang*, Tian Zhang*, Jianhua Zhao*, and Xuandong Li*

*Nanjing University, †The Hong Kong Polytechnic University
Outline

- Motivation
- Examples
- Offline Modeling and Verification
- Online Periodical Modeling and Verification
- Conclusion
Outline

- Motivation
- Examples
- Offline Modeling and Verification
- Online Periodical Modeling and Verification
- Conclusion
Motivation

- Cyber-Physical System: Hybrid
- Safety-Critical Applications
- Hybrid Systems Model Checking: Verifiably Safe
Laser Tracheotomy MDPnP

- SpO2 sampling period: 1 second

Safety Rule:
- Cannot shoot laser when patient’s windpipe O2 level is high!
Train Control System

- Train communicate with RBC for new MA by 500ms.
- If a train’s SBD tip point reaches MA border, normal brake!
- If a train gets no updates from RBC for 5s, emergent brake!

Safety Rule:
- No Collision During Emergent Braking!
Outline

- Motivation
- Examples
- Offline Modeling and Verification
- Online Periodical Modeling and Verification
- Conclusion
Challenges

- Difficult To Model
  - Offline

- Difficult To Verify:
  - Composed System
  - State Space Explosion
  - Nonlinear Function
  - High Complexity
Inhale (ventilator pumps out):

\[ \dot{O}_2(t) = b - a_{in\text{hale}}O_2(t); \]
\[ S\dot{O}_2(t) = ?. \]

Hold (ventilator holds):

\[ \dot{O}_2(t) = -a_{\text{hold}}O_2(t); \]
\[ S\dot{O}_2(t) = ?. \]

Exhale (ventilator pumps in):

\[ \dot{O}_2(t) = -a_{\text{exhale}}O_2(t); \]
\[ S\dot{O}_2(t) = ?. \]
Train Control System

Radio Block Center
Challenges

- **Difficult To Model**
- **Offline**

- **Difficult To Verify:**
  - Composed System
  - State Space Explosion
  - Nonlinear Function
  - High Complexity
Outline

- Motivation
- Examples
- Offline Modeling and Verification
- Online Periodical Modeling and Verification
- Conclusion
Proposed Solution: periodical online modeling and verification of time-bounded behavior.

- Difficult To Model Offline → Easy to Model Online

- Difficult To Verify ➔ Easy to Verify
  - Many configuration variables become fixed constants
  - Time-bounded future behaviors
  - Nonlinear behavior becomes linear
Laser Tracheotomy MDPnP

- Verified By PHAVer, Only 0.27 seconds < 1 second
Proposed Solution: periodical online modeling and verification of time-bounded behavior.

- **Difficult To Model Offline** ➔ Easy to Model Online
- **Difficult To Verify** ➔ Easy to Verify
  - Many configuration variables become fixed constants
  - Time-bounded future behaviors
  - Nonlinear behavior becomes linear
Train Control System

- No need to build model for RBC,
- 3 Trains, Verified by BACH, Only 58 ms<<500ms!
- Motivation
- Examples
- Offline Modeling and Verification
- Online Periodical Modeling and Verification
- Conclusion
Conclusion

- Online Periodical Modeling and Verification
- Time-Bounded Behavior
- Fast Real-Time Verification
Contact:

Lei Bu: bulei@nju.edu.cn
Qixin Wang: csqwang@comp.polyu.edu.hk
http://www.comp.polyu.edu.hk/~csqwang

Presentation Video URL:
http://www.youtube.com/wchshapp
Thanks

Q&A