Towards Formal Analysis of Cyber-physical Systems Security

George Louthan John Hale
Nathan Singleton Mauricio Papa

The University of Tulsa
Institute for Information Security

Overview

- Background: Hybrid and Cyber-physical Systems
- Challenges and opportunities
- State of the Field
- Our Approach
- Research Plan
- Outcomes

- Hybrid System
  - System with discrete and continuous components
  - Governed by digital logic and differential equations
- Cyber-physical System
  - Networked hybrid system
  - Examples:
    - Medical monitoring
    - Autonomous vehicles
    - Distributed robotics
    - Critical infrastructure

Challenges and Opportunities

- Theory
  - CPS include both discrete and continuous components
  - Systems composed by networks
- Simulation
- Metrics

State of the Field

- Hybrid Automata (Alur, Henzinger, et al.)
  - Labeled state transition system
  - Continuous *flow conditions*
  - Discrete *init* and *jump conditions*
  - Strengths: Well-studied and fitted to real systems
  - Weaknesses:
    - High dimensionality quickly leads to intractability
    - No topological (network-like) composition
- Others
  - Hybrid I/O Automata (Lynch)
  - Hybrid Process Algebra (Bergstra, et al.)

Our Approach

- Study "real" systems
  - Model systems we can build and run in our lab
  - Critical infrastructure
  - Automotive
- Integrate network communication into hybrid automata composition
- Study how changes in the "cyber" portion of CPS influence real world

Research Plan

- Identify suitable formalism for network modeling
- Fix target application domain
  - Automotive, critical infrastructure, medical
  - Linear, elliptical, etc. differential equations in continuous space
- Select desired analytical properties of the system
- Build network composition framework

Outcomes

- Formal theoretical framework for modeling CPS
- Execution model or simulation environment
- Metrics specifications
- Niche checking/audit tools
  - Field-deployable application to make FM-backed reports about its environment

Conclusion

Problem	Need to model cyber-physical systems
Prior Work	Focuses on isolated hybrid systems
Opportunities	Unfilled niche for comprehensive formal CPS model
Our role	Unite hybrid systems and networking formalisms
Main message	**Model the network**