Specification, Design and Verification of Distributed Embedded Systems

Mani Chandy    John Doyle    Richard Murray
California Institute of Technology

Eric Klavins    Pablo Parrilo
U. Washington    MIT

2007 V&V MURI Kickoff
7 August 2006
Goals and Agenda

Goals

• Provide an overview of the planned activities and approach of the MURI
• Provide a brief introduction to some of the technologies we will build on
• Describe the strategy for transitioning results to industry and government partners

Agenda

1:45 MURI overview (Murray)
2:15 Specification and Reasoning Using Graph Grammars (Klavins)
2:35 Integrating Continuous & Discrete Domains for Distributed Systems (Chandy)
2:55 Break
3:15 Proof Systems in Continuous and Discrete Domains (Parrilo)
3:35 Complexity Implies Fragility (Doyle)
3:55 Transition Strategy (Murray)
4:15 Discussion and Feedback (Wells/Heise)
Motivation: Transportation and Aerospace

Themes
- Autonomy
- Real-time, global dynamic interconnectivity
- Ultra-reliable systems; embedded software
- Multi-disciplinary teams
- Modeling for control
  - more than just $\dot{x} = f(x, u, p, w)$
  - analyzable accurate hybrid models

Technology Areas
- Air traffic control, vehicle management
- Mission/multi-vehicle management
- Command and control, human in the loop
- Ground traffic control (air & ground)
- Automotive vehicle & engine control
- Space vehicle clusters
- Autonomous control for deep space travel
Integration of computer science, communications, and control

- Time scales don’t allow standard abstractions to isolate disciplines
- Example: how do we maintain a consistent, shared view of the field?

Higher levels of decision making and mixed initiative systems

- Where do we put the humans in the loop? what do we present to them?
- Example: predict “plays” by the other team, predict next step, and react
Networked Control Systems

(following P. R. Kumar)

- Optimization-based framework for estimation and navigation
- Higher level decision-making to guide overall behavior
- Very few tools for design above the inner loop and individual module levels
V&V MURI Team

Principal Investigators

• Mani Chandy (Caltech CS)
• John Doyle (Caltech CDS)
• Gerard Holzmann (JPL CS)*
• Eric Klavins (U. Washington, EE/CS)
• Richard Murray (Caltech CDS)
• Pablo Parrilo (MIT EE)

Partners

• Air Force Research Laboratory: IF, MN, VA, VS
• Boeing Corporation - Systems of Systems Integration
• Honeywell Corporation - Guidance and Control
• Jet Propulsion Laboratory (JPL) - Laboratory for Reliable Software (LARS)
Problem Scope

Overall Goal:
Develop methods and tools for designing control policies, specifying the properties of the resulting distributed embedded system and the physical environment, and proving that the specifications are met

Specification
• How does the user specify---in a single formalism---continuous and discrete control policies, communications protocols and environment models (including faults)?

Design and reasoning
• How can engineers reason that their designs satisfy the specifications?
• In particular, can engineers reason about the performance of computations and communication, and incorporate real-time constraints, dynamics, and uncertainty into that reasoning?

Implementation
• What are the best ways of mapping detailed designs to hardware artifacts, running on specific operating systems? What languages are suitable for specifying systems so that the specifications can be verified more easily?
Program Thrusts

Specification and Reasoning Using Graph Grammars
• Build on Klavins’ Computation and Control Language (CCL) & SPIN (Holzmann)
• Use graph grammars to define interaction rules and reason about them

Sum of Squares Techniques (SOS)
• Unified framework for finding invariants and proof certificates for nonlinear and hybrid systems

Extensions
• Probabilistic techniques (specification + algorithms)
• Adversarial settings (including security issues)
• Computational techniques (with JPL/CACR)

Testbeds
• Caltech Multi-Vehicle Wireless Testbed (hardware + sims)
• Alice: 2005 and 2007 DARPA Grand Challenge entry
Transition Strategy

Toolbox development
• Develop and disseminate algorithms via publicly available toolboxes (DESTOOLS)

Annual workshops/short courses
• Model after mutools workshops developed by Balas, Doyle and Packard
• Provide opportunity for researchers to learn about the toolboxes developed under the MURI and apply the design tools to simple problems
• Provide forum for feedback to MURI team and discussion of needed tools
• Develop new courses and new course materials that can be used to teach students the required background to be effective practitioners and researchers in distributed embedded systems

Personnel exchange
• Student internships at AFRL labs and industry
• Industry visitors: eg, Sonja Glavaski from Honeywell spending 1 month at Caltech

Additional workshops and tutorials
• Connections II: Foundations of Network Science, 14-18 Aug @ Caltech
• CDC 2006: High Confidence Embedded Systems (Klavins and Murray)
Yearly Goals and Milestones

Year 1
- Extend existing work on graph grammars and SOS to allow temporal logic and nonlinear (hybrid) dynamics to co-exist
- Version 2.0 of SOSTOOLS, including preliminary temporal logic analysis tools
- Initial implementation of specification & design language, with manual guided proofs
- First annual workshop on V&V for Distributed Systems (Caltech)

Year 2
- Automated proof techniques for deterministic specifications
- Version 1.0 of distributed embedded systems toolbox (DESTOOLS)
- Second annual workshop on V&V for Distributed Systems (MIT)

Year 3
- Probabilistic descriptions of specifications, combined with underlying tools
- Version 2.0 of DESTOOLS: probabilistic descriptions
- Short course notes/research monograph describing framework, theory, and tools
- Third annual workshop on V&V for Distributed Systems (CDC or ACC)
Goals and Agenda

Goals

• Provide an overview of the planned activities and approach of the MURI ✔
• Provide a brief introduction to some of the technologies we will build on
• Describe the strategy for transitioning results to industry and government partners

Agenda

1:45 MURI overview (Murray)
2:15 Specification and Reasoning Using Graph Grammars (Klavins)
2:35 Integrating Continuous & Discrete Domains for Distributed Systems (Chandy)
2:55 Break
3:15 Proof Systems in Continuous and Discrete Domains (Parrilo)
3:35 Complexity Implies Fragility (Doyle)
3:55 Transition Strategy (Murray)
4:15 Discussion and Feedback (Wells/Heise)