V&V MURI
Transition Strategy

Mani Chandy John Doyle Richard Murray
California Institute of Technology

Eric Klavins
U. Washington

Pablo Parrilo
MIT

Annual Review
27 October 2008

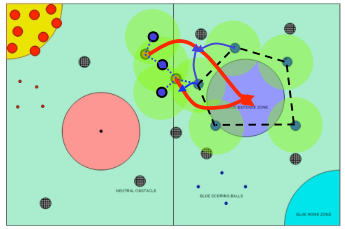
Problem Scope (Aug 06)

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

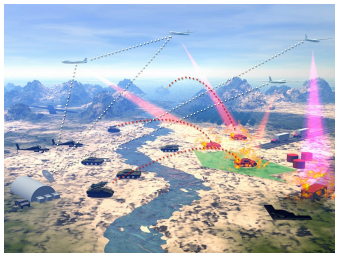
Specification

- 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?

Transition Goals and Approach (Aug 06)

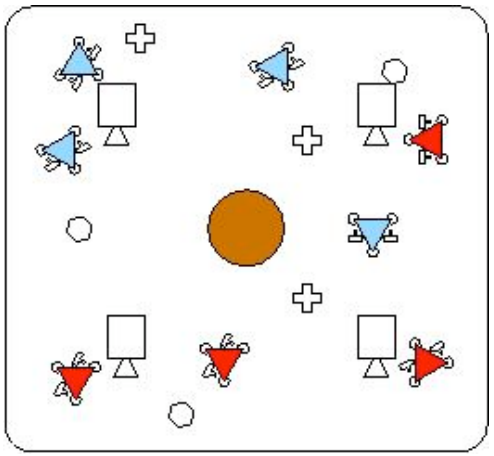
Goals

- Develop fundamental concepts and tools that get integrated into engineering tools
  - Focus the MURI on specification, design and reasoning (6.1)
  - Utilize partnerships with industry and govt labs to transition to implementation
  - Examples: mutools and SOSTOOLS
- Incorporate feedback from government and industry researchers and practitioners
  - Provide mechanisms for rapid testing of concepts with partners
  - Helps shape research directions to be consistent with most pressing needs

Approach

- Implementation on MVWT and Alice testbeds
- DESTOOLS - Distributed embedded systems toolbox
- Annual workshops and short courses
- Personnel exchange
- Integration with 6.2 and 6.3 efforts

Testbeds



Alice: An Information Rich System for Autonomous Navigation

- Data rich, networked control system: ~3 Gb/s raw data rates, 12 CPU processing
- Representative of level of complexity of UAV and other autonomous systems
- Using 2007 DGC results as case study for new V&V tools (Wongpiromsarn, Mitra)

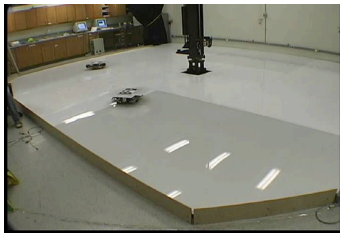
Caltech Multi-Vehicle Wireless Testbed (MVWT) + UW Programmable Parts Testbed

- Verify cooperative control strategies for multi-agent systems
- UW-MPP: implementation testbed for embedded graph grammars
- MVWT: new common NCS infrastructure to allow easier experimentation & testing

Distributed Embedded Systems Toolbox (Aug 06)

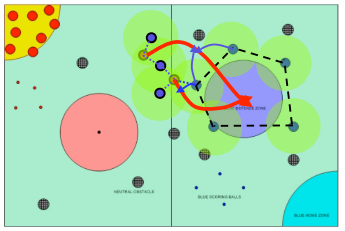
Version 1.0 (Year 2)

- Initial implementation of specification & design language (CCL++)
- Automated proof techniques for deterministic specs (SPIN++)



Version 2.0 (Year 3)

- Probabilistic descriptions of specifications, combined with underlying tools

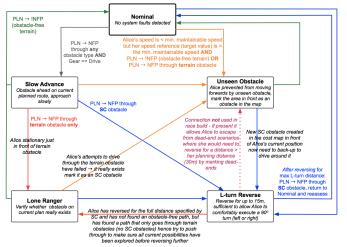


Version 3.0 (Year 4)

- Adversarial descriptions of the operational environment
- Applications of techniques from random algorithms
- Evaluation of scalability to industrial-scale problems

Version 4.0 (Year 5)

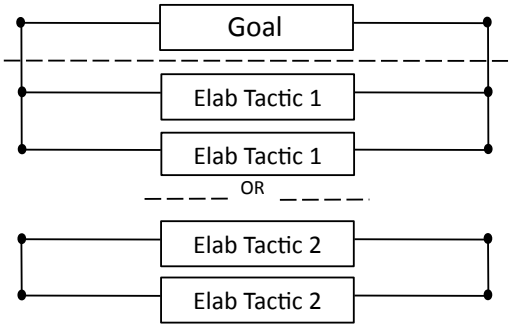
- Inclusion of security considerations through adversarial modeling
- Large scale computing support



Software Tools

Mission Data System (MDS) → Hybrid Automata

- Conversion of goal network to hybrid automata that can be verified using PHAVer, SPIN, etc
- Joint work with JPL, applying to Titan mission

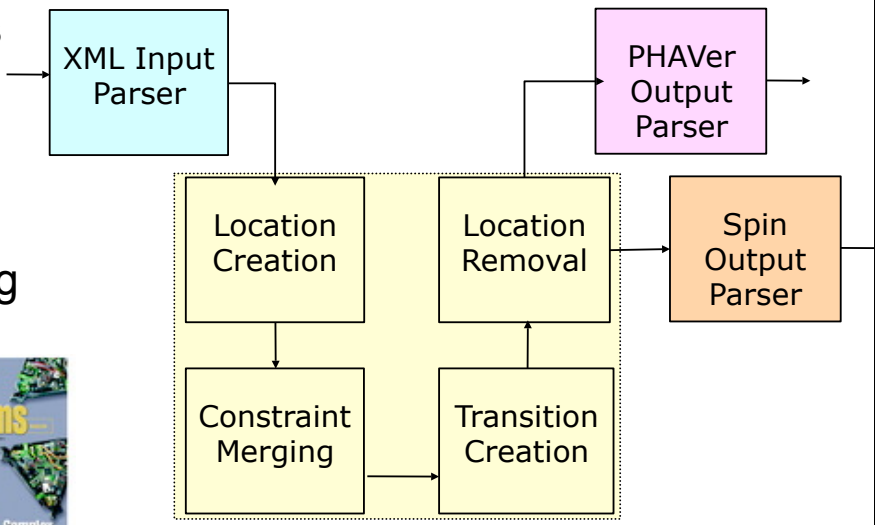


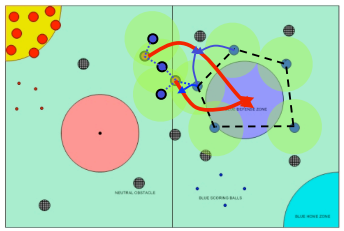
PVS metatheory for asynchronous iterative processes (Mitra et al)

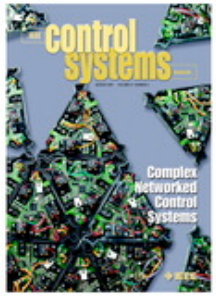
- "Library" for reasoning about stability in PVS
- Being used for verifying multi-robot protocols

NCS implementation tools (from DGC07)

- Open source tools available via sourceforge
- Implementing on MVWT for faster prototyping
- Sparrow, falcon, skynet, CCL







Annual Workshops, Short Courses, Course Materials

Public workshops/meetings

- CDC 06 - High Confidence Embedded Systems
- [Oct 08 - MIT cooperative control and game theory workshop]
- Oct 08 - Second annual MURI review

Courses and course materials

- Algebraic Techniques and Semidefinite Optimization (Parrilo; Caltech & MIT)
- Three term V&V sequence taught by JPL instructors (including G. Holzmann)
- SOSTOOLS incorporated into Caltech CDS 210 (first year grad controls course)
- Online distributed systems course being developed by Chandy (PVS, SPIN)

Personnel Exchanges and Interactions

Exchanges between Caltech, MIT and UW

- January 07: MVWT fest - Caltech + UW week long MVWT "festival"
- 2007-08: Danielle Tarraf - Joint MIT/Caltech postdoc (3 mo @ MIT, then CIT)
- Fall 2008: Pablo Parrilo visit + course at Caltech
- April 2008: David Thorsley visit to Caltech
- October 2008: MIT workshop on cooperative control/game theory (Murray to MIT)
- November 2009: Murray/Klavins trip to Boeing

Interaction with industry (Boeing), government (JPL, AFRL)

- Sonya Glavaski: annual visits while at Honeywell; restablishing ties via Eaton
- Julia Braman: ~bi-monthly meetings with JPL systems engineering group (MDS)
- Sean Callahan (Boeing): semi-annual visits to Caltech; Nov 09 trip to Boeing
- [Eugene Lavretsky (Boeing): spring course on adaptive control/system ID]
- Richard Murray: participation in AFRL/RBCC Flight Critical Systems and Software Initiative (FCSSI) Executive Panel (Graybeard) Review, Apr 08
- Gerard Holzmann (JPL): teaching CS 118 (model checking) + interactions with Mani Chandy, Julia Braman
- JPL: Three term V&V course sequence at Caltech
- Possible future interactions: UTRC, Eaton

Personnel Supported

Alumni

Aaron Ames	Postdoc, Caltech	Asst Prof, Texas A&M
Michel Charpentier	Visiting Prof, Caltech	Prof, U New Hampshire
Michael Epstein	Graduate student, Caltech	McKinsey
Melvin Flores	Graduate student, Caltech	JPL
Zhipu Jin	Graduate student, Caltech	Cisco
JM McNew	Graduate student, U Wash	Toyota
Sayan Mitra	Postdoc, Caltech	Asst Prof, UIUC
Ling Shi	Graduate student, Caltech	Asst Prof, HKUST
Demetri Spanos	Graduate student, Caltech	Visiting Asst Prof, USC
Danielle Tarraf	Postdoc, MIT/Caltech	Asst Prof, Johns Hopkins

Current project team (2008-09)

- 5 faculty (3 CIT, 1 MIT, 1 UW)
- 9 grad students (6 CIT, 2 MIT, 1 UW)
  - 4 women, 0 URM
- Anticipate 2-4 new grad students
- 1 postdoc (1 UW)
- Leveraged funding (Boeing): 1 postdoc, 4 grad students at Caltech

Deviations from Original Plan

More focus on fundamental theory versus tools and transition

- Toolboxes and workshops have not happened as quickly as originally planned
- Balanced by more work on fundamental mathematics and theory
  - Pulled work on probabalistic systems from year 3 into year 2
  - Pulled work on adversarial actions (game theory) from year 3/4 into year 2/3

Annual workshops not yet implemented

- Ran “kickoff” workshop at 2006 CDC, followed by internal workshops
- Tools are not yet at the point where a more general workshop seems fruitful
- Starting to see infrastructure develop; expect public workshop in summer 2009

Difficult to identify students to spend time at AFRL

- Originally hoped to send 2-3 students/summer to visit AFRL (multiple sites)
- US students often have many opportunities (JPL, industry, universities)
- Non-US students have some barriers and limited motivation

Plans for Years 3-5

Year 3

- Probabilistic descriptions of specifications, combined with underlying tools
- Initial implementation of specification & design language, with manual guided proofs
- Version 1.0 of distributed embedded systems toolbox (DESTOOLS)
- [Version 3.0 of networked control systems API (sparrow, falcon, skynet, CCL)]
- Second workshop on V&V for Distributed Systems (summer 2009)

Year 4

- Adversarial descriptions of the operational environment
- Applications of techniques form random algorithms and large scale computation
- Version 2.0 of DESTOOLS: probabilistic descriptions
- Third workshop on V&V for Distributed Systems (summer 2010)

Year 5

- Inclusion of security considerations through adversarial modeling
- Version 3.0 of DESTOOLS: adversarial interactions
- Short course notes/research monograph describing framework, theory, and tools