Specification, Design and Verification of Distributed Embedded Systems

Mani Chandy John Doyle Richard Murray (PI)
California Institute of Technology

Eric Klavins
U. Washington

Pablo Parrilo
MIT

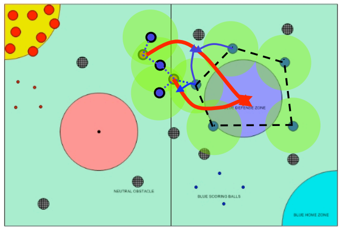
Future Directions
September 2009

Problem Scope

Overall Goal:

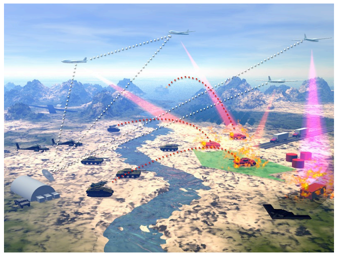
Develop methods and tools for designing control policies, specifying the properties of the resulting distributed embedded system and the physical environment, and proving that the specifications are met

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?

Transition Strategy

Workshops, tutorials and courses

- CDC 2006: High Confidence Embedded Systems (Klavins and Murray)
- Hands-on workshop @ Caltech, 16-17 Sep 09 - PVS, LTV, PHAVer and more
- V&V research workshop @ Caltech, 23-24 Sep 09 - external speakers (U. Topcu)
- Contemplating ACC 2010 or CDC 2010 workshop
- New verification courses at Caltech (Chandy + Topcu)

Toolbox development

- Develop and disseminate algorithms via publicly available toolboxes
  - CCL, (SPIN), PVS toolboxes, SBT Checker/Inveriant
  - [SOS-based toolboxes (Topcu, Packard et al)]

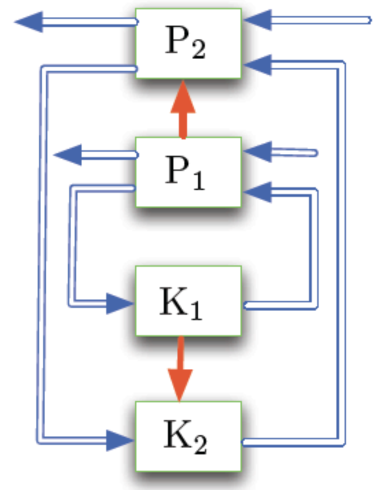
Papers (2006 - present)

- 9 journal papers (+3 submitted): IEEE TAC, P. IEEE, Distributed Computing, J. DSMC
- 33 conference papers: ACC, CDC, FORMATS, HSCC, AIAA

People

- 24 graduate students, 5 postdocs, 1 visiting professor
- Alumni placement: university (5), industry (3), government lab (2)
- Multiple visits between sites (Caltech, MIT, UW) + additional joint activities

Accomplishments and Lessons



Lyapunov (-like) functions continue to be a powerful tool

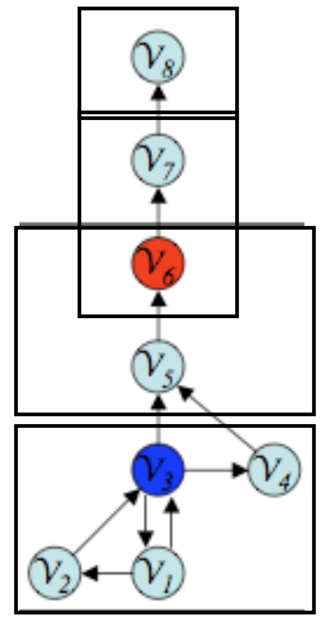
- Allows us to reason about entire sets of continuous variables
  - system properties → algebraic conditions
- Can also capture problems in discrete transition systems
  - lexicographically-ordered Lyapunov fcns for graph grammars
- Powerful new tools (based on SOS) are making reasoning easier
  - non-monotonic Lyapunov functions, ROA estimates, ...

Use temporal logic for specification at higher levels of abstraction

- Allows descriptions of proper behavior on execution *sequences*
- Model checking/theorem proving provide tools for verifying behavior
  - PVS, SPIN, TLC, SBT Checker/Inveriant, TLV, ...
- "LTL should be part of every control engineer's knowledge basis"

Asynchronous behavior via guarded command languages

- Guarded command languages allow good description of distributed operation with no globally synchronized clock
- Can reason about asynchronous behavior using LTL formalisms
- CCL with rates to describe stochastic, multi-rate systems



Opportunities for Future Research

Great progress on V&V over the past 3+ years (two MURIs + lots of other work)

- Still many good opportunities for research
- DARPA RFI SN-09-67 (3 Sep 09) - Paul Eremenko, TTO
- We should also continue thinking about fundamental aspects (next MURI?)

Stochastic specification, design and composition

- Some initial work within the MURI on stochastic systems (rates of failure, etc)
- Much more work to be done on how to design the distributions for stochastic systems
- How can we compose faulty systems with high level monitors to provide better performance guarantees than the underlying components?

Correct-by-construction design methods for hybrid systems

- Can we go directly from specifications to closed loop protocols (ala RHC)?
- Advances in exploring paths for LTL-specified systems gives some hope
- Need better way to plan at different levels of abstraction in a protocol stack (ala nets)

Grand Challenge problems for verification (AFRL?, DARPA?)

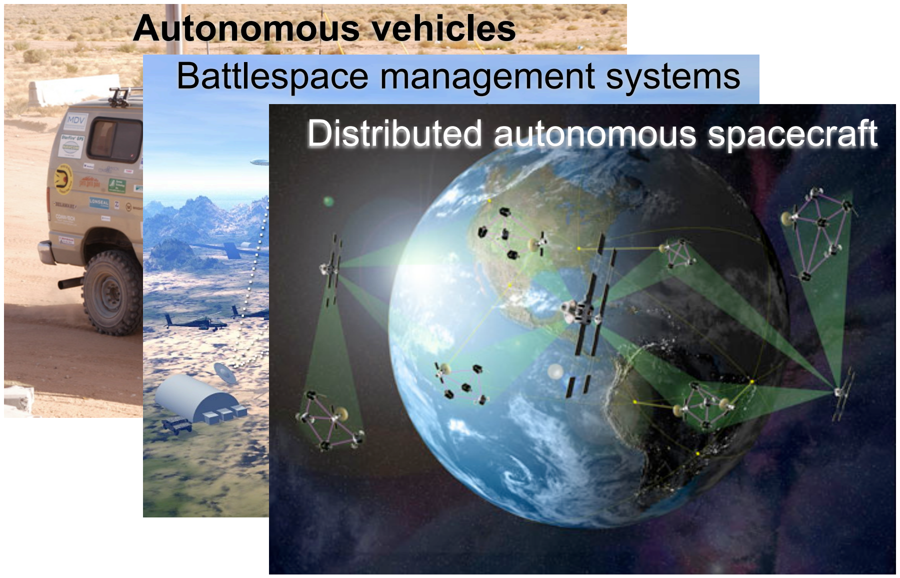
- Develop a "grand challenge" style problem, with advancement to round two depending on the ability to verify the system design
- Use results to develop a set of "best approaches" for 2020 Air Force systems

2008 Review Feedback

- Great MURI
- Good theory; most very impressive
- Not clear how it all tied into one picture
  - Was this a single MURI with everyone particating toward a single goal?
  - Might have just been an issue of presentation
- Less connection between U Washington and Caltech/MIT
- Would like to see PIs/students come out to the labs and get things connected up
- Students seemed really engaged; recognized where the funding was coming from
- Course development seems good; good training for students
- Toolbox: different people felt differently
- Would be nice to define "robustness"; sometimes unclear what that means
- How does the environment play into V&V; won't come out of stochastic games

Specification, Design and Verification of Distributed Embedded Systems

Caltech/MIT/UW, Murray (PI)/Chandy/Doyle/Klavins/Parrilo



Long-Term PAYOFF: Rigorous methods for design and verification of distributed systems-of-systems in dynamic, uncertain, adversarial environments

OBJECTIVES

- Specification language for continuous & discrete control policies, communications protocols and environment models (including faults)
- Analysis tools to reason about designs and provide proof certificates for correct operation
- Implementation on representative testbeds

APPROACH/TECHNICAL CHALLENGES

- Specification and reasoning using guarded command languages, temporal logic and graph grammars
- Sum of squares analysis for certificates, invariants
- Model checking/theorem proving for hybrid systems
- Extensions to probabilistic, adversarial and networked operations

ACCOMPLISHMENTS/RESULTS

- Foundations of local/global properties of computation
- Embedded graph grammars for cooperative control
- Lyapunov-based verification of temporal properties
- Receding horizon temporal logic planning
- New formulations of game theory/stochastic problems

FUNDING ($K)—Show all funding contributing to this project

	FY06	FY07	FY08	FY09	FY10	FY11
AFOSR Funds	417	1000	1000	1000	1000	593
Boeing	310	390	390	370	[390]	
DARPA GC		1200				

TRANSITIONS

- Application to autonomous driving (DGC07)
- Software toolkits, workshops, and personnel transfer

STUDENTS, POST-DOCS

2006-09: 24 graduate students, 5 postdocs, 4 undergraduates

LABORATORY POINT OF CONTACT

Dr. Siva Banda, AFRL/RBCA, WPAFB, OH