CPS – Breakthrough: Development of Novel Architectures for Control and Diagnosis of Safety-Critical Complex Cyber-Physical Systems

Stéphane Lafortune and Necmiye Ozay **Department of EECS, University of Michigan**

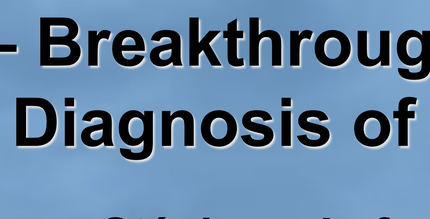
Overall Objective:

•Scalability of formal methods for synthesis of provably-correct controllers

•Development of abstraction techniques that lift CPS design problem to synthesis problem on discrete state system

•Combination of control and fault diagnosis to ensure resilience and adaptivity

•Consideration of the distributed features of the system at synthesis step and at implementation step



Project Start Date:
January 2015

Project Website:
https://wiki.eecs.umich.edu/complexcps/

Participants:

• Graduate Students

Xiang Yin, Yun Jae Cho, Yunus Sahin

• Undergraduate Students

Dylan Lawton, Stanley Smith, Siyuan Shen, Andrew Wagenmaker

Industrial Collaborators:

• UTC Aerospace Systems (UTAS)

• Ford Motor Company

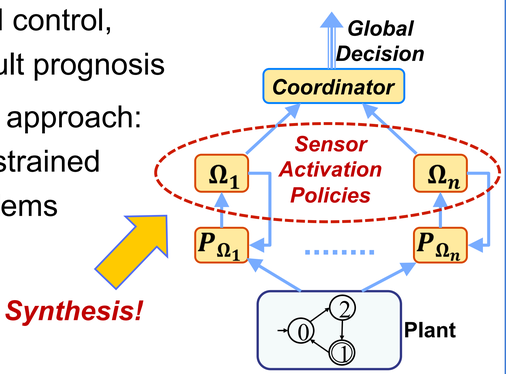
Recent Results:

• Controller Synthesis

- A uniform information-state-based approach: synthesis based on two-player game; bipartite transition systems (BTS)
- Properties Considered: safety, opacity, diagnosability, attractability, etc.
- Two stages when solving game: first enforce IS-based property, then enforce non-blockingness
- Range control problem: minimal behavior guaranteed
- Software: DPO-SYNT

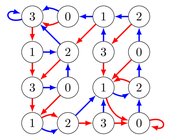
• Synthesis of Sensor Activation Policy

- We leverage the IS-based approach to solve the sensor activation problem
- Both centralized and decentralized synthesis problem
- Problem Considered: decentralized state disambiguation problem, e.g., decentralized control, fault diagnosis, fault prognosis
- Person-by-person approach: solve a set of constrained minimization problems



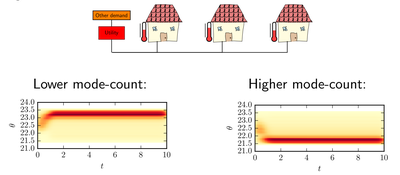
• Scalable Abstraction Algorithms

- Structural properties: large # of systems, small # of classes; counting constraints (sufficiently many/not too many); identity of individual systems is not important
- An abstraction-based control synthesis method that
  - exploits symmetry (permutation invariance) in dynamics and specifications
  - works across scales (10 to 10K or more systems)
- Several applications: scheduling thermostatically controlled loads, multi-agent system coordination



10000 TCL units, each with 2 modes:

$$\dot{\theta}_i = -a(\theta_i - \theta_a) - bP_m$$



- Simulation equivalence instead of bisimulation
- Overlapping partitions: hierarchical by construction, convexity preserving, improved termination guarantees

Selected Publications:

1.X. Yin and S. Lafortune. "A uniform approach for synthesizing property-enforcing supervisors for partially-observed discrete-event systems," *IEEE Transactions on Automatic Control*, 61(8): 2140-2154, 2016.

2.X. Yin and S. Lafortune. "Synthesis of maximally permissive supervisors for partially observed discrete event systems," *IEEE Transactions on Automatic Control*, 61(5): 1239-1254, 2016.

3. P. Nilsson and N. Ozay, "Control synthesis for large collections of systems with mode-counting constraints", 19th International Conference on Hybrid Systems: Computation and Control (HSCC), Vienna, April 2016.

4. A. Wagenmaker and N. Ozay, "A bisimulation-like algorithm for abstracting control systems", Proc. Allerton Conference on Communication, Control, and Computing, Monticello, IL, September 2016.

UNIVERSITY OF MICHIGAN

DISCRETE EVENT SYSTEMS GROUP
UNIVERSITY OF MICHIGAN