COLLEGE OF ENGINEERING, UC BERKELEY

http://chess.eecs.berkeley.edu/superb/

SUPERB-IT

Center for Hybrid and Embedded Software Systems

Tool for Probabilistic Safety Verification of Stochastic Hybrid Systems

Author: *Nandita Andromeda Mitra, Rutgers University*
Mentors: *Saurabh Amin and Alessandro Abate*

Abstract

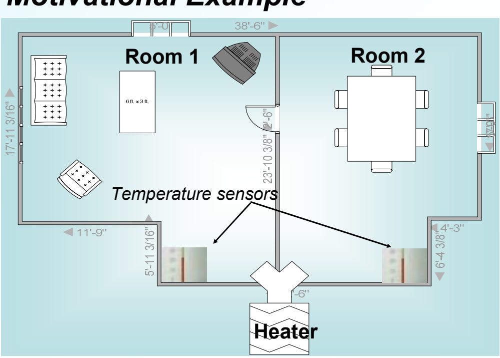
Many safety critical systems like air traffic control involve modeling their behavior as *hybrid systems*. The effect of uncertain system dynamics and external inputs can be incorporated by modeling the system as a controlled stochastic hybrid system (SHS). Design of controllers for SHS that guarantees a certain safety criterion can be posed as a quantitative verification problem. The goal of this project is to develop a computational tool for stochastic reachability analysis of a benchmark SHS.

Introduction

Stochastic hybrid systems (SHS) model probabilistic uncertainty in hybrid systems. An important problem in SHS is probabilistic reachability:

- With what probability the system can reach a certain set during some time horizon?
- (If possible), select a *control input* to ensure that the system remains outside the set with *sufficiently high* probability
- When the set is unsafe, the problem becomes a *quantitative safety verification* problem.

Motivational Example

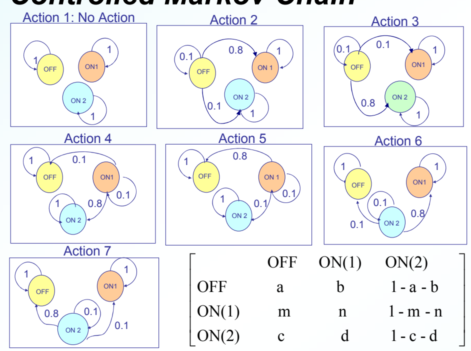


- **Temperature in two rooms is controlled by one heater. Safe set for both rooms is 20 – 25 (^{0}F).**
- **Goal is to keep the temperatures within corresponding safe sets with a high probability.**
- **SHS model**
  - -Two continuous states: x_1, x_2
  - -Three modes: OFF, ON (Room 1), ON (Room 2)
  - - Continuous evolution in mode ON (Room 1)

$$x_1(k+1) = x_1(k) + \{\alpha_1(x_a - x_1(k)) + \alpha_c(x_2(k) - x_1(k)) + k_1\}\Delta t + n_1(k)$$
$$x_2(k+1) = x_2(k) + \{\alpha_1(x_a - x_2(k)) + \alpha_c(x_1(k) - x_2(k))\}\Delta t + n_2(k)$$

  - -Mode switches defined by controlled Markov chain with seven discrete actions.

Controlled Markov Chain



	OFF	ON(1)	ON(2)
OFF	a	b	1 - a - b
ON(1)	m	n	1 - m - n
ON(2)	c	d	1 - c - d

Typical Transition Matrix

Maximal Probabilistic Safe set Computation

For safety level $(1-\epsilon)$, the maximal safe set

$$S^* = \{s \in \mathcal{S} : \inf_{\mu \in \mathcal{M}_m} P_s^{\mu}(A) \le \epsilon\}$$

Dynamic programming (DP) recursion

Define the functions $V_k^*: \mathcal{S} \to [0,1]$ by

$$V_N^*(s) = 1_{A^c}(s)$$
$$V_k^*(s) = \sup_{(u,\sigma)\in\mathcal{U}\times\Sigma} 1_{A^c}(s)\int_{\mathcal{S}} V_{k+1}^*(s_{k+1}) T_s(ds_{k+1}|s,(u,\sigma)), \text{ for } k \in [0, N-1]$$

Then, $V_0^*(s) = 1 - \inf_{\mu\in\mathcal{M}_m} P_s^{\mu}(A)$ for all $s \in \mathcal{S}$ so,

$$S^* = \{s \in \mathcal{S} : V_0^*(s) \ge 1-\epsilon\}$$

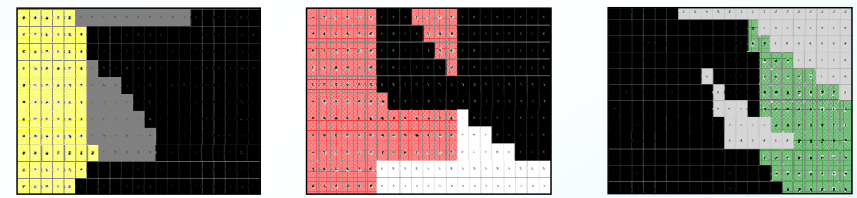
Optimal policy is shown to be

$$\mu_k^*(s) = \arg\sup_{(u,\sigma)\in\mathcal{U}\times\Sigma} 1_{A^c}(s)\int_{\mathcal{S}} V_{k+1}^*(s_{k+1}) T_s(ds_{k+1}|s,(u,\sigma))$$

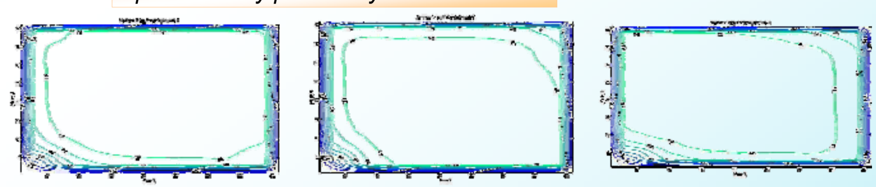
Results

Stochastic DP implemented for time horizon of 150 minutes using time step of 1 minute and spatial discretization of 0.25 ^{0}F.

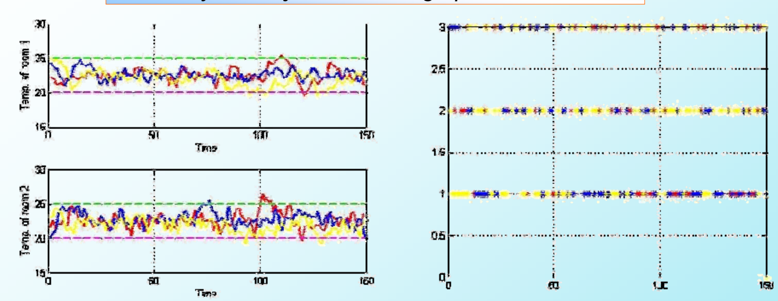
Optimal actions for 149th minute and three modes



Optimal safety probability for three modes



Three hybrid trajectories using optimal control law



Conclusions and Future Work

- Implemented stochastic DP algorithm with multiplicative cost function for computing probabilistic maximal safe sets and optimal feedback policy for probabilistic safety verification of a two-room thermostat modeled as a controlled discrete time SHS.
- Future work will include efficient implementation of stochastic DP for multi-room, multi-heater case to address computational issues.
- Application to other applications such as air traffic control.

SUPERB-IT Final Poster Session

Acknowledgements: Dr. Jonathan Sprinkle, Prof. Shankar Sastry, **CHESS, SUPERB, Family and Friends**

Berkeley UNIVERSITY OF CALIFORNIA

August 4, 2006