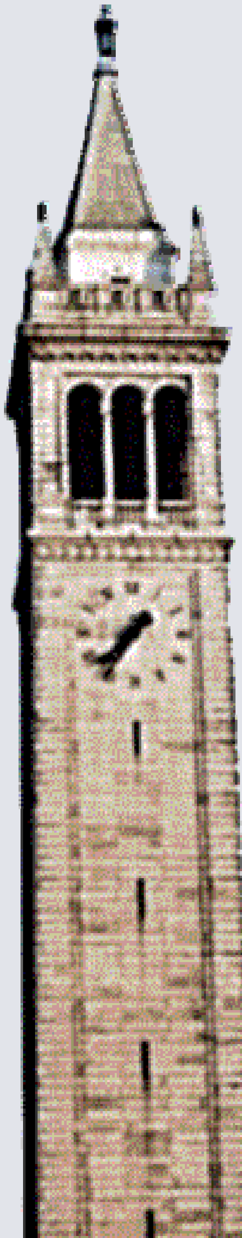
Reachability Analysis for Discrete Time Stochastic Hybrid Systems

Edited and presented by

Saurabh Amin

UC Berkeley



Chess Review

November 21, 2005

Berkeley, CA

Introduction

- Stochastic hybrid systems (SHS) can model uncertain dynamics and stochastic interactions that arise in many systems
- Probabilistic reachability problem:
  - What is the probability with which the system can reach a set during some finite 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. In this case, find the *maximal safe sets* corresponding to different safety levels

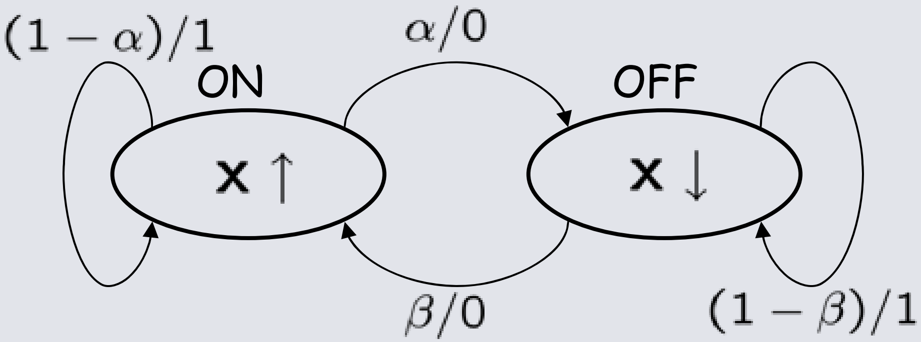
Discrete Time Stochastic Hybrid System (DTSHS)

- Definition of DTSHS $\mathcal{H} = (\mathcal{Q}, n, \mathcal{U}, \Sigma, T_x, T_q, R)$
  where $\mathcal{Q}$ is the set of modes, the map n defines the dimension of the continuous state space of these modes, $\mathcal{U}$ and Σ are the transition and reset control spaces, and T_x, T_q , and R are continuous, discrete, and reset stochastic kernels
- DTSHS as controlled Markov process
  - State space: $\mathcal{S} = \cup_{q \in \mathcal{Q}} \{q\} \times \Re^{n(q)}$
  - Control space: $\mathcal{A} = \mathcal{U} \times \Sigma$
  - Controlled transition kernel: $T_s(ds'|s,(u,\sigma))$ which is

$$T_x(dx'|(q,x),u)T_q(q'|s,u) \quad \text{if } q' = q \text{ (no transition)}$$
$$R(dx'|(q,x),\sigma,q')T_q(q'|s,u) \quad \text{if } q' \neq q \text{ (transition)}$$

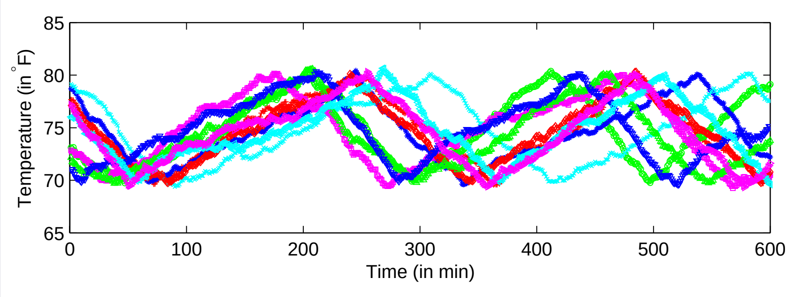
Motivational Example

Thermostat



Trivial Switching Control Law

Switch when state hits unsafe set



- System dynamics
  - Continuous dynamics
    - OFF $\mathbf{x}(k+1) = a\mathbf{x}(k) - C_1 + \mathbf{n}(k)$
    - ON $\mathbf{x}(k+1) = a\mathbf{x}(k) + C_2 + \mathbf{n}(k)$
  - Discrete transition kernel
    - "Switch" $\begin{pmatrix} 1-\alpha & \alpha \\ \beta & 1-\beta \end{pmatrix}$
    - "Don't switch" $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
  - Continuous and reset transition kernels
    - Off $\mathcal{N}(\cdot; ax - C_1, \nu^2)$
    - ON $\mathcal{N}(\cdot; ax + C_2, \nu^2)$

Stochastic Reachability

- Assumptions
  - Markov policies
    - Set $\mathcal{M}_m$ of $\mu = (\mu_0, \ldots, \mu_{N-1}) \ni \mu_k : \mathcal{S} \to \mathcal{A}$
  - Finite horizon and complete observability
- Reach Probability
  - Probability that the execution of $\mathcal{H}$ associated with policy $\mu \in \mathcal{M}_m$ and initial distribution π will enter set A during time $[0, N]$

    $p_\pi^\mu(A) = P_\pi^\mu(\mathbf{s}(k) \in A \text{ for some } k \in [0, N])$
- Probabilistic safe set
  - Set that guarantees safety probability $(1 - \epsilon)$ for policy $\mu \in \mathcal{M}_m$: $S^\mu(\epsilon) = \{s \in \mathcal{S} : p_s^\mu(A) \leq \epsilon\}$

Backward Reachability Computations

- Multiplicative cost function
  - Note that $p_\pi^\mu(A) = 1 - p_\pi^\mu(A^c)$
  - Where, $p_\pi^\mu(A^c) = E_\pi^\mu[\prod_{k=0}^{N} \mathbf{1}_{A^c}(\mathbf{s}(k))]$
- Reach probability computation by backward recursion for fixed Markov policy μ
  - Define the set of functions $V_k^\mu : \mathcal{S} \to [0,1]$ as

$$\begin{aligned} V_N^\mu(s) &= \mathbf{1}_{A^c}(s) \\ V_k^\mu(s) &= \mathbf{1}_{A^c}(s) \int_{\mathcal{S}} V_{k+1}^\mu(s_{k+1}) T_s(ds_{k+1}|s,(\mu_k(s)), \text{ for } k \in [0, N-1] \end{aligned}$$

  - Then, $p_\pi^\mu(A^c) = \int_{\mathcal{S}} V_0^\mu(s)\pi(ds)$
  - And, $S^\mu(\epsilon) = \{s \in \mathcal{S} : V_0^\mu(s) \geq 1 - \epsilon\}$

Maximal Probabilistic Safe Set Computation

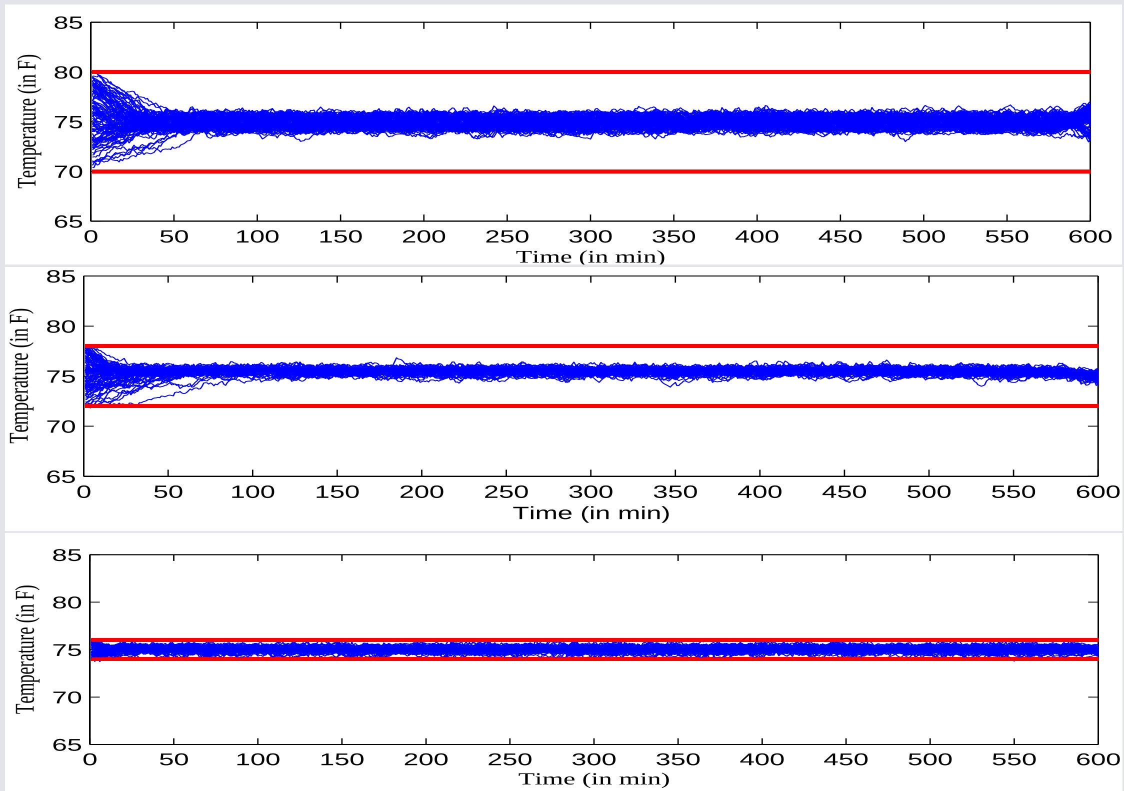
- For safety level $(1-\epsilon)$, maximal safe set
  $S^* = \{s \in \mathcal{S} : \inf_{\mu \in \mathcal{M}_m} p_s^{\mu}(A) \leq \epsilon\}$
- Dynamic programming recursion
  - Define the set of functions $V_k^* : \mathcal{S} \to [0,1]$ as

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

  - Then, $V_0^*(s) = 1 - \inf_{\mu \in \mathcal{M}_m} p_s^{\mu}(A)$ for all $s \in \mathcal{S}$
  - And so, $S^* = \{s \in \mathcal{S} : V_0^*(s) \geq 1 - \epsilon\}$
- Existence of optimal policy

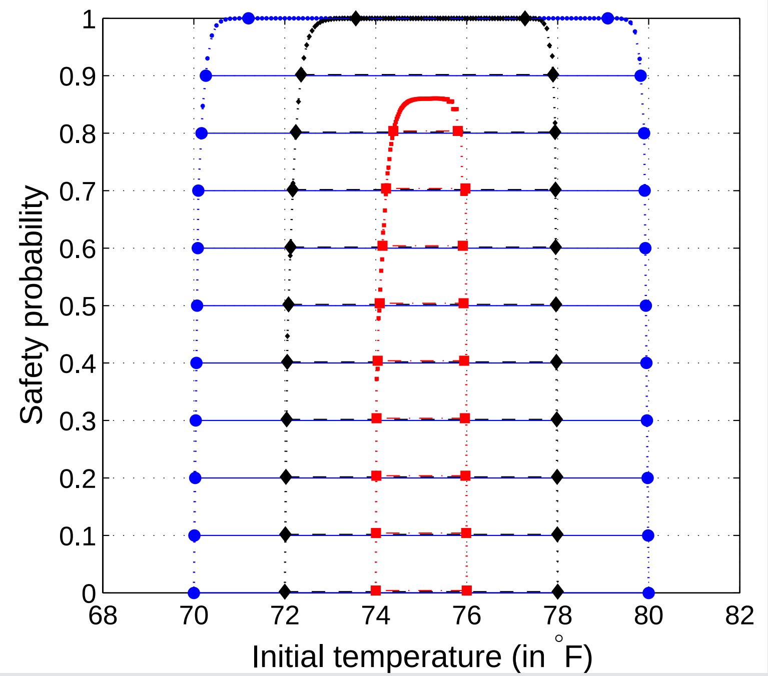
$$
\mu_k^*(s) = \arg\sup_{(u,\sigma) \in \mathcal{U} \times \Sigma} \mathbf{1}_{A^c}(s) \int_{\mathcal{S}} V_{k+1}^*(s_{k+1}) T_s(ds_{k+1} | s, (u,\sigma))
$$

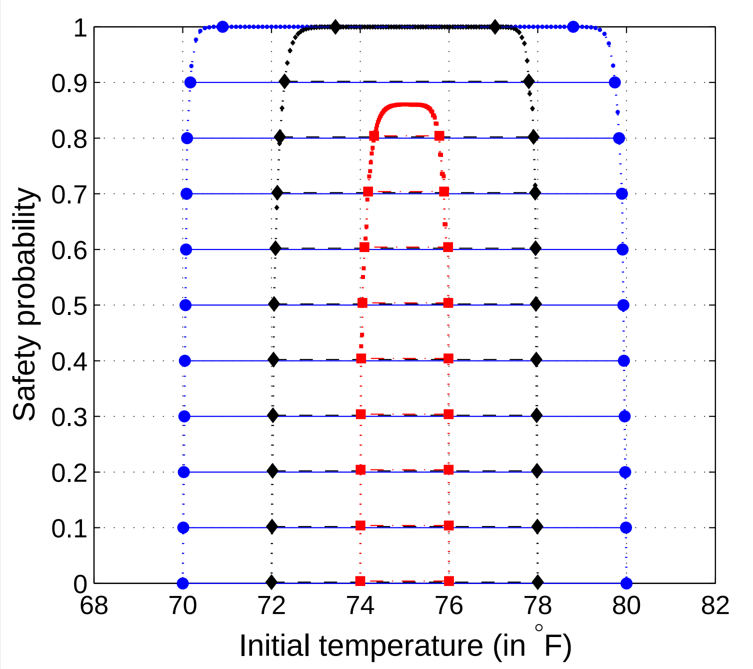
Computational Results (1/3)



- Executions generated by optimal policy for three safe sets: $(70, 80)^{\circ}F, (72, 78)^{\circ}F$ and $(74, 76)^{\circ}F$

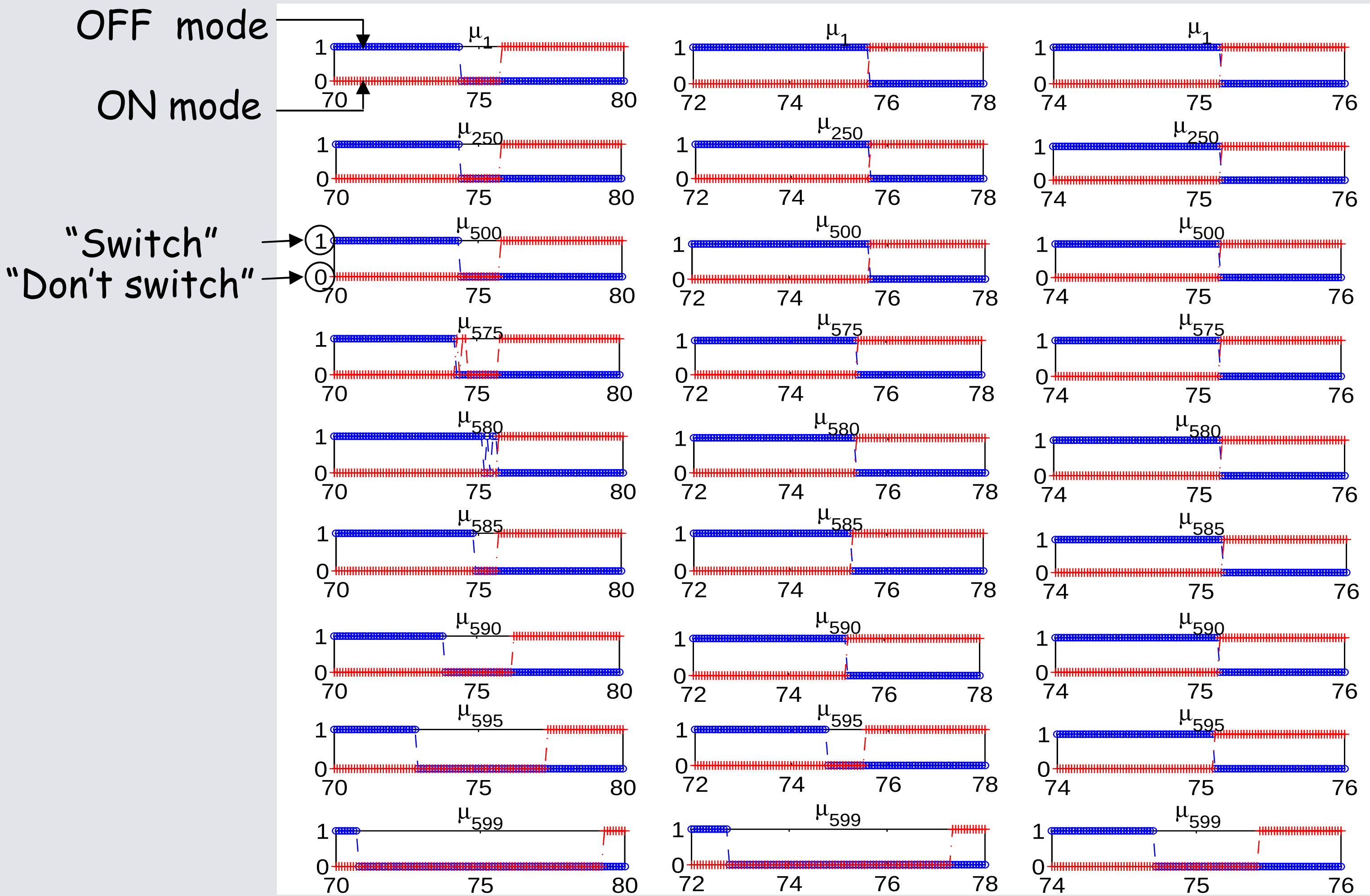
Computational Results (2/3)





- Maximal probabilistic safe sets for the three sets for different safety levels when the initial mode of heater is “OFF” and “ON” respectively

Computational Results (3/3)



- Optimal control policy in "OFF" and "ON" modes for the three sets as a function of temperature at different times

Conclusion and Future Work

- For controlled SHS
  - Proposed a model for controlled discrete time SHS suitable for optimal control and reachability analysis
  - Interpreted the safety verification problem in terms of stochastic reachability notion
  - Developed a dynamic programming based approach for computing probabilistic maximal safe sets and the optimal feedback policy
  - Applied the proposed methodology on a simple example and presented computational results
- Future work
  - To address the problem of reachability analysis for continuous time SHS