Tool for probabilistic safety verification of stochastic hybrid systems

Nandita Andromeda Mitra
Electrical Engineering
Rutgers, the State University of New Jersey
nanda@eden.rutgers.edu

Graduate Mentor: **Saurabh Amin and Alessandro Abate**
Research Supervisor: **Dr. Jonathan Sprinkle**
Faculty Mentor: **Prof. S. Shankar Sastry**

August 4, 2006

Summer Undergraduate Program in
Engineering Research at Berkeley (SUPERB) 2006

Department of Electrical Engineering and Computer Sciences
College of Engineering
University of California, Berkeley

Tool for probabilistic safety verification of stochastic hybrid systems

Nandita Andromeda Mitra

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.

1 Introduction

Hybrid systems can be found in many systems: air traffic control, epidemiology, biological networks, population dynamics. Hybrid dynamical models(systems having both continuous and discrete dynamics) can describe these systems efficiently. But there can be incidents when the system dynamics are not deterministic and that will lead us to their stochastic nature. Reachability analysis and safety verification are two crucial problems in hybrid system theory. Reachability analysis is finding out if for a specific initial condition, a given system will reach a set or not and safety verification is estimating the probability of reaching or not reaching that set. More research on this topic can be found in [2],[3],[5],[6]. This project deals with discrete time stochastic hybrid system(DTSHS)[2], that has a control input.The system consists of two room and one heater. Dynamic programming has been used to calculate the probability of its remaining in a safe set. Following to subsections will give the readers a clear idea of hybrid systems.

1.1 Hybrid System : A non-deterministic example

To understand hybrid systems first we need to know about dynamical system. Briefly dynamical system describes how states changes in the course of time. So we can think of two kind of dynamical systems: Continuous(when states take real values in the Euclidean Space) and Discrete(when state takes integers). But we can think of another phenomenon where both continuous and discrete systems are related. That is how the concept of hybrid system comes. So dynamical system involving continuous time dynamics and discrete time dynamics is hybrid dynamics. In other words it can be said as discrete program in an analog environment. Though it can be a combination of other dynamics, we will deal with only this combination. We will use discrete "jumps" to specify changes in the discrete states and differential equations to express the changes in continuous states. Continuous states can change through jumps too. Hybrid system can be deterministic and stochastic. We will concentrate in stochastic hybrid system(SHS) in this report.

A good starting example of non-deterministic hybrid system is the thermostat example. We want to control the temperature of a room using a controller. The controller consists of a radiator which is controlled by a thermostat. So when the thermostat is OFF the temperature goes exponentially toward zero:

$$\dot{x} = -rx, \qquad where \qquad r > 0 \tag{1}$$

When the thermostat is ON the temperature of the room increases according to another differential equation:

$$\dot{x} = -r(x - T), \qquad T = any\, temperature \tag{2}$$

We can try to make a controller that will keep the temperature of the room around 50 degree. So if the temperature rises above 51 degree the heater will turn off and if it goes below 49 degree the heater will turn on. We can add some uncertainty saying in both case the heater can remain unchanged till 52 degree and 48 degree respectively.

It is noticeable that the system has both continuous and discrete state. The temperature of the room is the continuous part, $x \in \mathbb{R}$ and $q \in \{ON, OFF\}$ is the discrete state.

1.2 Hybrid system : A stochastic example

Stochastic hybrid systems are affected by uncertainty. So the new thing we will add here is the concept of probability. so we will use *Stochastic Differential Equation* for continuous dynamics and *Markov Chain* for discrete dynamics. Stochastic analysis helps us to improve the performance of embedded system with uncertainty. Safety require performance of an embedded system also needs analysis of stochastic hybrid systems. We can use our thermostat example to explain Stochastic Hybrid System. In this case the switch will follow the command according to some probability. If the discrete transition is T_q we can make the following two models:

$$T_q(q'|(q,x),0) = \begin{cases} 1, q' = q \\ 0, q' \neq q \end{cases}$$

$$T_q(q'|(q,x),1) = \begin{cases} a, & q' = \text{OFF}, q = \text{ON} \\ 1-a, & q' = q = \text{ON} \\ b, & q' = \text{ON}, q = \text{OFF} \\ 1-b, & q' = q = \text{OFF} \end{cases}$$

Here, $a \in [0,1]$ is the probability of switching from the ON mode to OFF mode in one time step. Similarly, $b \in [0,1]$. We assume that there is a time step between the actual switching of the heater. During this time step the temperature keeps evolving according to the dynamics referring to the starting condition.

1.3 Outline of the report

Section 2 introduces wiener process to explain the noise we have used in the model. Section 3 will introduce Euler-Maruyama method of discretization. Section 4 will explain the model of controlling temperature of two rooms using one heater. Section 5 will be the conclusions and future work.

2 Wiener Process:

Wiener process or brownian motion is continuous time dependent random variable. Stochastic differential equations are modeled using this concept. We will denote it as W(t). It has the following properties:

- W(t) has basic infinitesimal moments

$$\mathrm{E}[dW(t)] = 0 \text{ and } \mathrm{Var}[dW(t)] = dt$$

  with initial condition $W(0^+) = 0$ with probability one.

- W(t) has *independent increments.*

- It is a stationary process, as the distribution of the increment is independent of t.

- W(t) is a *Markov Process*. Since the value of W(t) for any $t \geq 0$ depends only on the present state.

- For $0 \leq s \leq t \leq T$ the increment $W(t) - W(s)$ is a normally distributed random variable. So we can write $W(t) - W(s) \sim \sqrt{t-s}N(0,1)$, where N(0,1) is a normally distributed random variable with zero mean and unit variance.

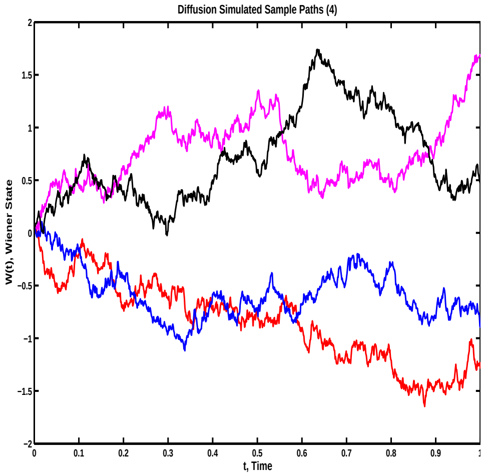


Figure 1. Four diffusion sample paths

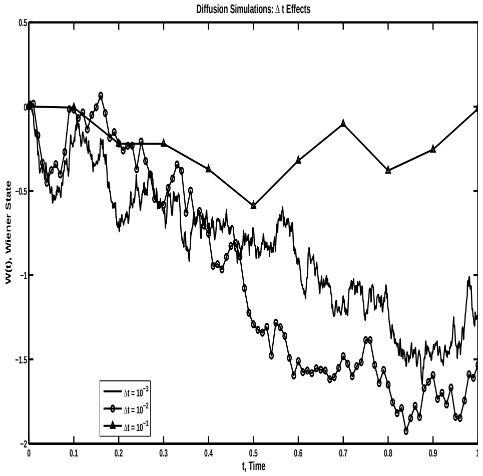


Figure 2. Wiener diffusion sample path using different time steps

In Fig: 1 four random wiener paths for $N = 1000$ and $T = 1$ has been shown. In Fig: 2 the diffusion paths for different N and Δt has been plotted.

3 Euler-Maruyama (EM) Method:

The Euler-Maruyam method is a numerical method for finding the solutions of a stochastic diffusion equation according to its definition of the Ito stochastic integral. If we have a scalar, automonous stochastic diffusion equation of the following form

$$X(t) = X_0 + \int_0^t f(X(s))ds + \int_0^t g(X(s)dW(s)), 0 \leq t \leq T \tag{3}$$

Here, f and g are scalar functions and X_0 is a random variable that gives the initial condition. Now we can write the above equation in differential form as

$$dX(t) = f(X(t))dt + g(X(t))dW(t), X(0) = x_0, 0 \leq t \leq T \tag{4}$$

To apply EM method we need the discretization interval, $\Delta t = T/L$. Here, L is a positive integer, and $\tau_j = j\Delta t$. Now the EM method takes the following form

$$X_j = X_(j-1) + f(X_(j-1))\delta t + g(X_(j-1))(W(\tau_j) - W(\tau_{j-1})), j = 1, 2, ..., L. \tag{5}$$

Each term in the right hand side of this equation is approximations of the corresponding term on the right hand side of equation 4. For more information about EM method please see [1].

4 Multi room Thermostat Example:

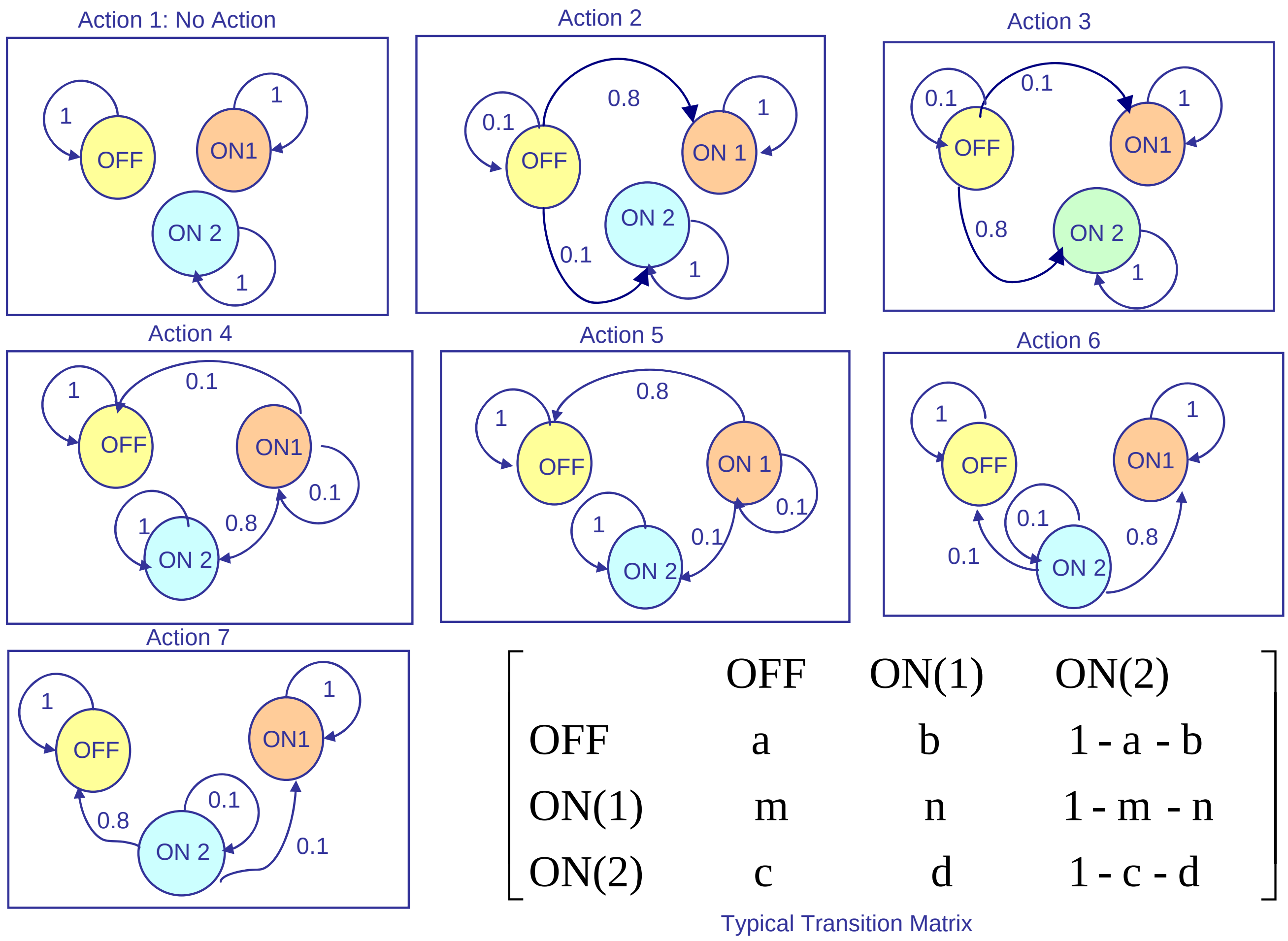
Now we are going to consider the case where we have two rooms but only one heater to control their temperatures. Our goal is to keep both the room temperature in desired intervals. In this case we have three discrete modes:

1. The heater is ON and it is facing room 1.(Will be denoted later as ON1)
2. The heater is ON and it is facing room 2.(Will be denoted later as ON2)
3. The heater is OFF.

And two continuous states:

1. Safe set for room 1 is from 20 degree to 25 degree.
2. Safe set for room 2 is from 20 degree to 25 degree.

In this case, mode switches are defined by controlled Markov chain with seven discrete actions. Those are shown in Fig: 3. Each action has its distinct transition matrix. Action 1 (which is no action) means we will stay in the state where we were. Action 1 is considering the case where we want to jump to ON1 from OFF with some probability(which is 0.8 in this case). So if the heater is OFF and the temperature of room one goes below 20 then the heater will start and turn to room one. With 0.1 probability it can stay in OFF mode or with 0.1



$$\left[\begin{array}{lccc} & \text{OFF} & \text{ON(1)} & \text{ON(2)} \\ \text{OFF} & a & b & 1 - a - b \\ \text{ON(1)} & m & n & 1 - m - n \\ \text{ON(2)} & c & d & 1 - c - d \end{array}\right]$$

Figure 3. The controlled markov chain of the two room example

probability it can face room two. But if it is in ON1 or ON2 it will stay there. The other actions work in the same way.

Now the average temperatures of the rooms can develop according to the following stochastic differential equation:

Heater is ON facing ROOM 1

$$dx_t^1 = \{\alpha_1(x_a - x_t^1) + \alpha_c(x_t^2 - x_t^1) + K_1\}dt + \gamma_1 dw_t^1 \tag{6}$$
$$dx_t^2 = \{\alpha_2(x_a - x_t^2) + \alpha_c(x_t^1 - x_t^2)\}dt + \gamma_2 dw_t^2 \tag{7}$$

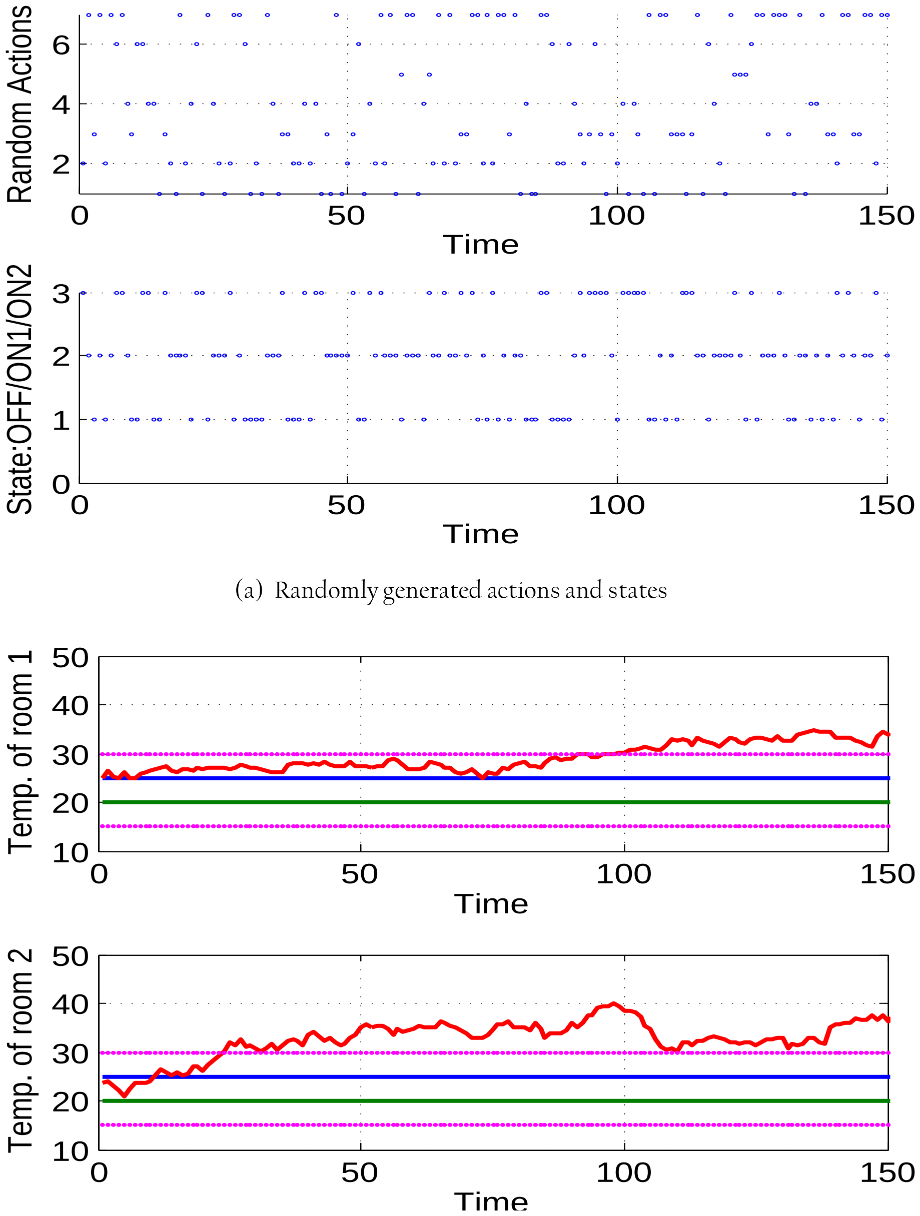
Heater is ON facing ROOM 2

$$dx_t^1 = \{\alpha_1(x_a - x_t^1) + \alpha_c(x_t^2 - x_t^1)\}dt + \gamma_1 dw_t^1 \tag{8}$$
$$dx_t^2 = \{\alpha_2(x_a - x_t^2) + \alpha_c(x_t^1 - x_t^2) + K_2\}dt + \gamma_2 dw_t^2 \tag{9}$$

Heater is OFF

$$dx_t^1 = \{\alpha_1(x_a - x_t^1) + \alpha_c(x_t^2 - x_t^1)\}dt + \gamma_1 dw_t^1 \tag{10}$$
$$dx_t^2 = \{\alpha_1(x_a - x_t^2) + \alpha_c(x_t^1 - x_t^2)\}dt + \gamma_2 dw_t^2 \tag{11}$$

Here, x_a is the ambient temperature. α_1 and α_2 are average heat loss rates and K_1 and K_2 are the rates of heat gain of room one and room two respectively. α_c is the coupling constant for both of the rooms. w(t)s are standard Wiener process model which represents the noise affecting the temperature evolution.γ is a constant related to the variance of the noise.



(a) Randomly generated actions and states

(b) Randomly generated temperatures for room 1 and room 2

Figure 4. Randomly generated information

Using Euler-Maruyama discretization rule to the SDEs mentioned in section 3 we get the stochastic difference equations. Here, the time step is Δt

Heater is ON facing ROOM 1

$$x_1(k+1) = x_1(k) + \{\alpha_1(x_a - x_1(k)) + \alpha_c(x_2(k) - x_1(k)) + K_1\}\Delta t + n_1(k) \tag{12}$$

$$x_2(k+1) = x_2(k) + \{\alpha_2(x_a - x_2(k)) + \alpha_c(x_1(k) - x_2(k))\}\Delta t + n_2(k) \tag{13}$$

Heater is ON facing ROOM 2

$$x_1(k+1) = x_1(k) + \{\alpha_1(x_a - x_1(k)) + \alpha_c(x_2(k) - x_1(k))\}\Delta t + n_1(k) \tag{14}$$

$$x_2(k+1) = x_2(k) + \{\alpha_2(x_a - x_2(k)) + \alpha_c(x_1(k) - x_2(k)) + K_2\}\Delta t + n_2(k) \tag{15}$$

OFF

$$x_1(k+1) = x_1(k) + \{\alpha_1(x_a - x_1(k)) + \alpha_c(x_2(k) - x_1(k))\}\Delta t + n_1(k) \tag{16}$$

$$x_2(k+1) = x_2(k) + \{\alpha_2(x_a - x_2(k)) + \alpha_c(x_1(k) - x_2(k))\}\Delta t + n_2(k) \tag{17}$$

where, $n_1(k)$ and $n_2(k)$ is a sequence of i.i.d. Gaussian random variables with zero mean and variance $\sigma = \frac{1}{\gamma^2}\Delta t$.

In Fig: 4(a) I have plotted some randomly generated actions for time $k \in [0, 150]$. we can see that the heater is taking different action and switching from one mode to other almost each step. And Fig: 4(b) shows the teperatures in the rooms based on these actions. it can be seen that the temperature of room 1 is outside of the desired set from the very beginning and temperature of room 2 outside of the safe set almost in the beginning. These are not desirable. We want our temperature to be in 20-25 in both the rooms.

Now we have applied some switching conditions in our system. So that if the temperature of any of the rooms started going out of the defined boundary the heater will take step so that it doesn't go out. This control is not the optimal control. It just orders the heater where to move if some specific conditions occur. Fig: 5(a) gives the actions and states for this switching system. We can say that we are staying in action 1 which is no action mode for most of our time, which is one of the goals. So the heater is stable. And from Fig: 5(b) we can say that the temperatures are in the requested interval. For some time window they are touching the boundary and for room 2 it was outside of the boundary for a little while. So our next aim is to find out the probability of their remaining in the boundaries and maximize it, which can be stated as reachability analysis and maximum safe set verification.

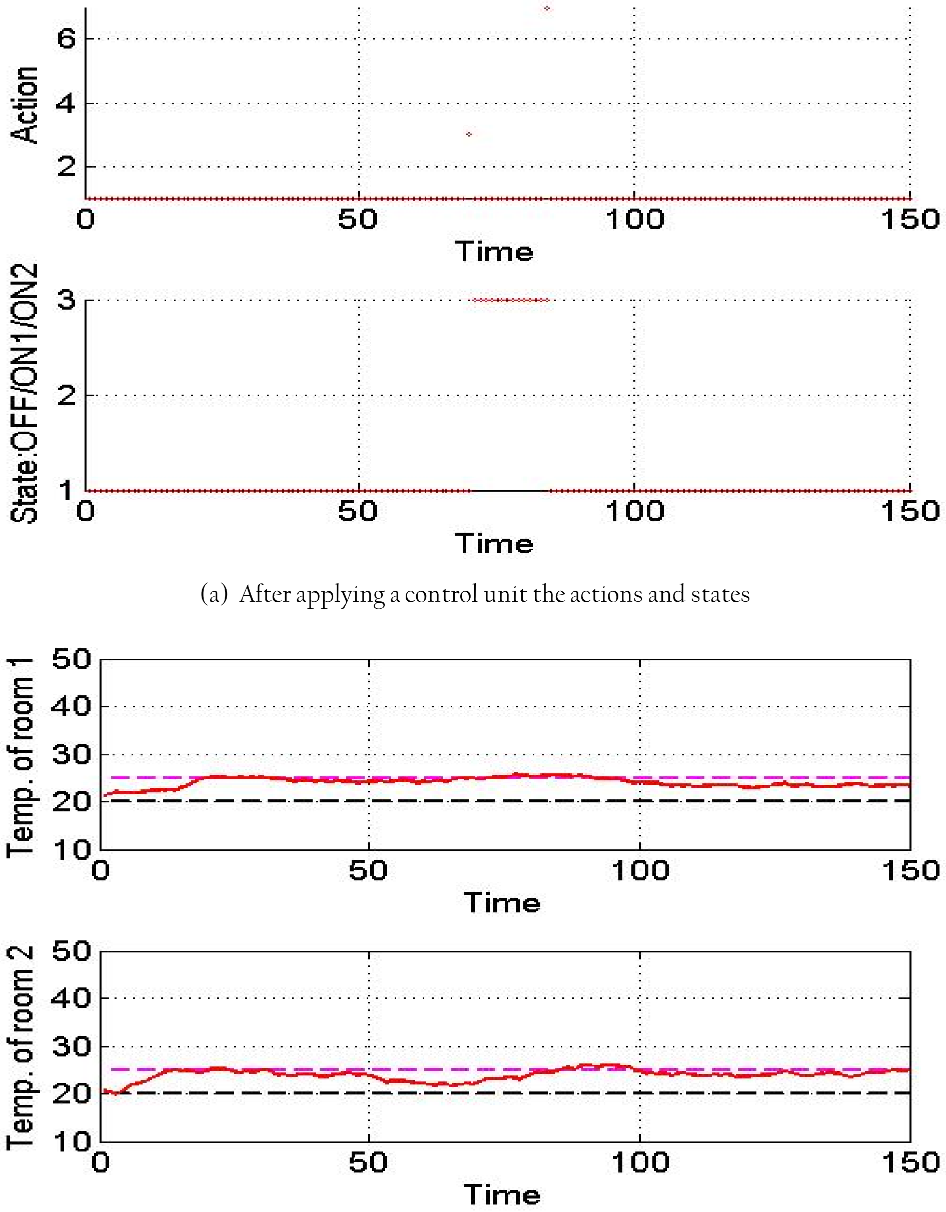
4.1 Stochastic Reachability

Probabilistic reachability problem:

1. What is the probability with which the system can reach a set during some finite time horizon? If the set is an unsafe set, then the problem becomes a safety verification problem.

2. (If possible), select control inputs to ensure that the system remains outside the set with sufficiently high probability.

Let A be the unsafe set for a system. Then the probability of entering the unsafe set can be written as following: $P^{\mu}_{\pi}(A) := P^{\mu}_{\pi}(s(k) \in A$ for some $k \in [0, N])$. Here, $\mu \in M_m$ is a Markov policy and π is the initial state distribution.



(a) After applying a control unit the actions and states

(b) After applying a control unit the temperatures for room 1 and room 2

Figure 5. After applying a control unit generated information

Now let assume the system has a probability of $\epsilon \in (0,1)$ of entering A, so the safety probability is $1-\epsilon$. The *probabilistic safe set* with safety level $1-\epsilon$ can be expressed as the following way

$S^{\mu}(\epsilon) = \{s \in \mathsf{S} : P^{\mu}_{\pi}(A) \leq \epsilon\}$

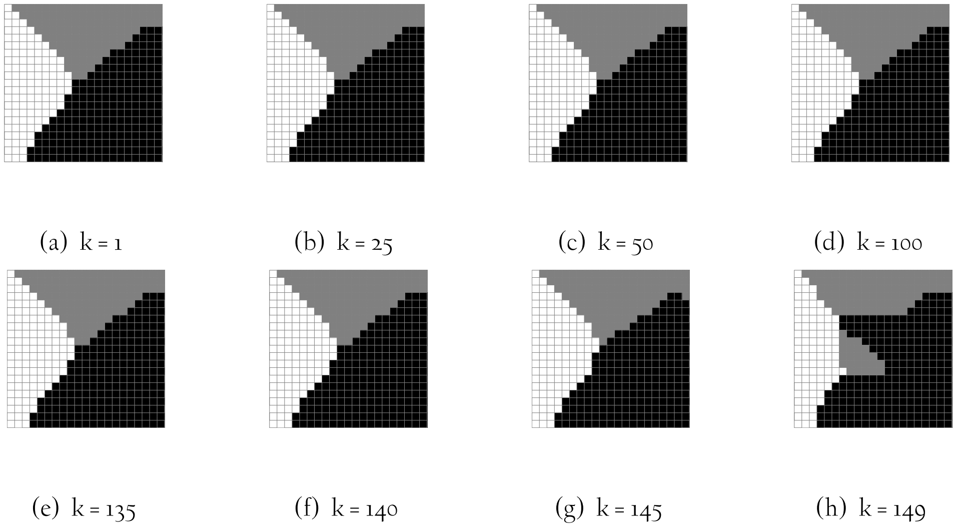
We have to maximize this probabilistic safe set.We can define $P^{\mu}_{\pi}(A)$ as $P^{\mu}_{\pi}(A) = 1 - p^{\mu}_{\pi}(\overline{A})$, where $\overline{A}$ denotes the complement of A in S. Now we can write the following equation:

$$p^{\mu}_{\pi}(\overline{A}) = P^{\mu}_{\pi}(\prod_{k=0}^{N} 1_{\overline{A}}(s(k)) = 1) = E^{\mu}_{\pi}(\prod_{k=0}^{N} 1_{\overline{A}}(s(k))) \tag{18}$$

Here, $1_{\overline{A}}(s)$ is an indicator function and $1_{\overline{A}}(s) = 1$ if $s \in \overline{A}$ and 0 otherwise. In this project $p^{\mu}_{\pi}(\overline{A})$ has been calculated using backward recursion. The probability of remaining outside of the unsafe set A during time interval $[k, N]$, with initial state s can be defined as:

$$V^{\mu}_{k}(s) = 1_{\overline{A}} \int_{\mathsf{S}} V^{\mu}_{k+1}(s_{k+1}) T_s(ds_{k+1}|s, \mu_k(s)) \tag{19}$$

And we have defined $p^{\mu}_{\pi}(\overline{A}) = V^{\mu}_{0}(s)$. As all the equations are taken from [2], interested readers are requested to see it for the mathematical proofs.


(a) k = 1

(b) k = 25

(c) k = 50

(d) k = 100

(e) k = 135

(f) k = 140

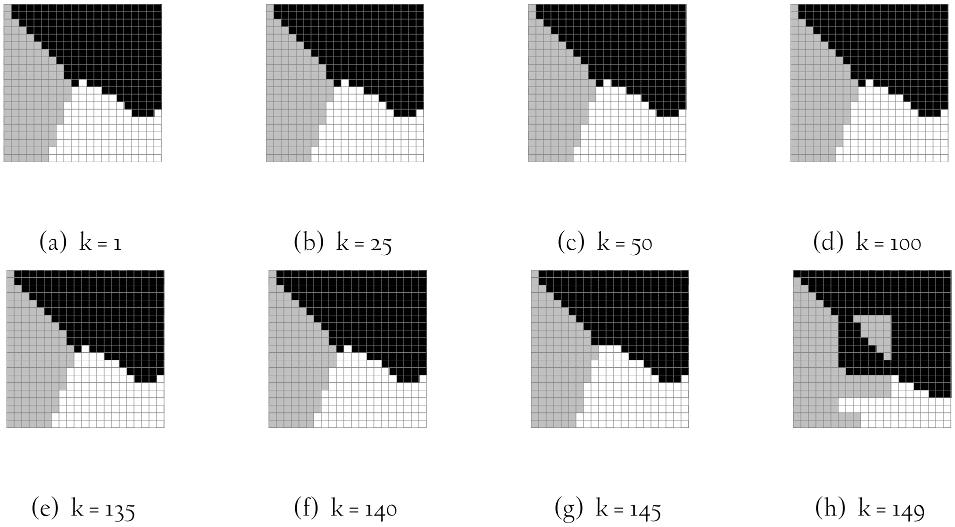
(g) k = 145

(h) k = 149

Figure 6. Some optimal actions taken by the heater for mode OFF. Here, black stands for action 1, gray is action 2 and white is action 3.In all the figures x-axis is the 21 discrete levels of the temperature of room 1 and y-axis is the 21 discrete levels of the temperature of room 2.

4.2 Results

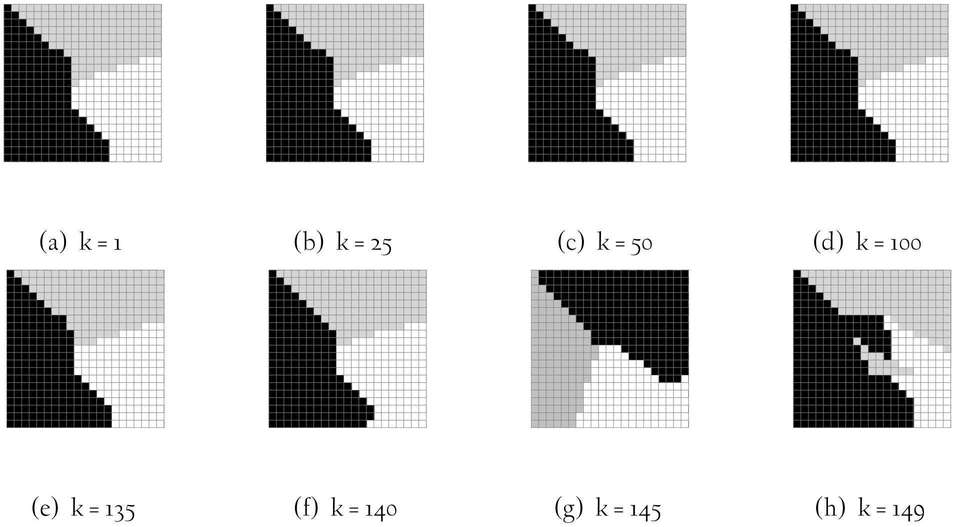
After applying the dynamic programming recursion mentioned above we got the maximally safe policies and maximal probabilistic safe sets. MATLAB has been used to do the implementations. The temperatures are discretized in 21 equally spaced values within the safe sets $[(20, 25)^oF]$ for both of the rooms. Time instances $k \in [0, 150], x_a = 6, \alpha_1 = 0.25, \alpha_2 = 0.25, K_1 = 12, k_2 = 14, \alpha_c = 0.33$, variance parameter of the noise, $\sigma = 0.9$. Some of these values are based on [4]. Following figures are the optimal actions taken by the heater in time steps $k \in [0, 150]$. The color in each box indicates the action taken which has been defined in Fig: 3.



(a) k = 1 (b) k = 25 (c) k = 50 (d) k = 100

(e) k = 135 (f) k = 140 (g) k = 145 (h) k = 149

Figure 7. Some optimal actions taken by the heater for mode ON1. Here, black stands for action 1, gray is action 4 and white is action 5. In all the figures x-axis is the 21 discrete levels of the temperature of room 1 and y-axis is the 21 discrete levels of the temperature of room 2

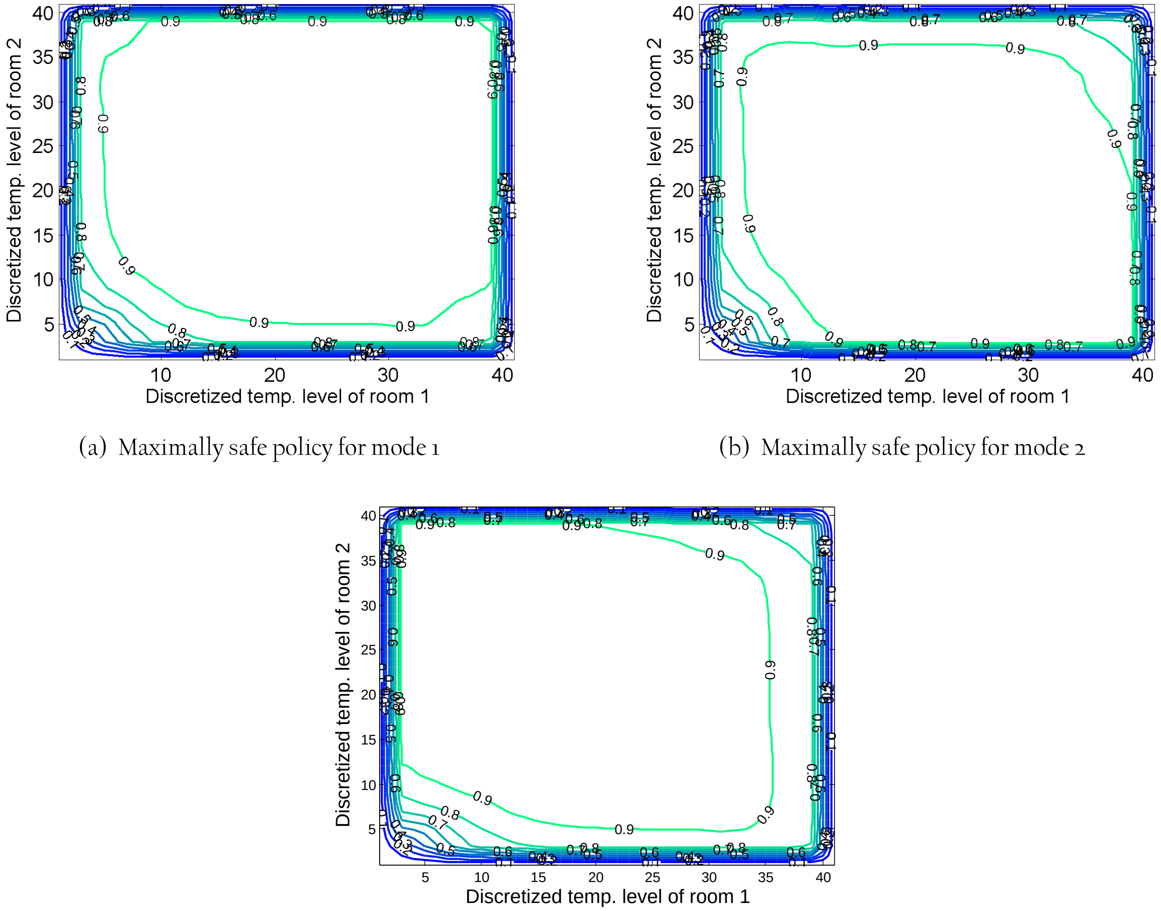


(a) k = 1 (b) k = 25 (c) k = 50 (d) k = 100

(e) k = 135 (f) k = 140 (g) k = 145 (h) k = 149

Figure 8. optimal actions taken by the heater for mode ON2. Here, black stands for action 1, gray is action 6 and white is action 7. In all the figures x-axis is the 21 discrete levels of the temperature of room 1 and y-axis is the 21 discrete levels of the temperature of room 2

From the figure we can see that the heater is taking the same actions for different time which means that the heater is not switching too much from one mode to another.



(a) Maximally safe policy for mode 1

(b) Maximally safe policy for mode 2

(c) Maximally safe policy for mode 3

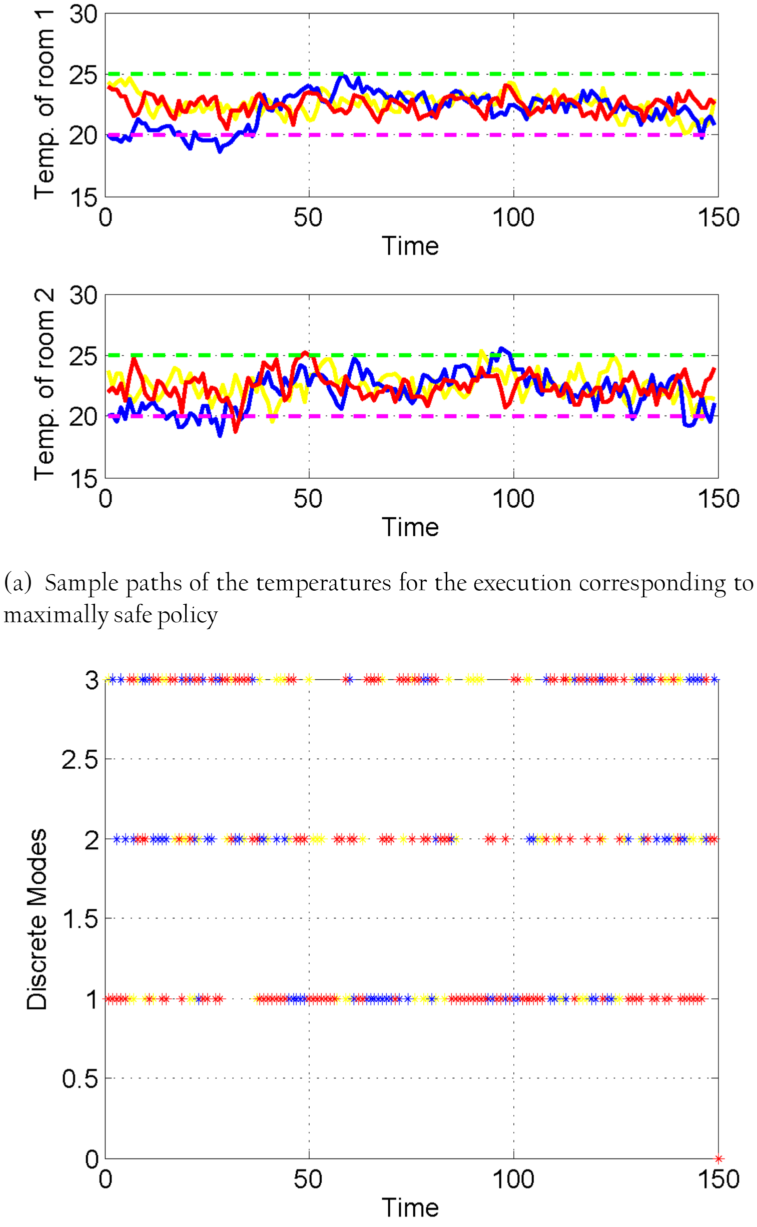
Figure 9. Optimal probabilistic safe sets

Figure 10(a) show the plots of the temperatures of the two rooms using the corresponding maximally safe policy. The initial operating mode has been chosen at random between the equiprobable OFF, ON1 and ON2 values. Figure 10(b) are the corresponding modes taken by the heater during the execution.

The maximal probabilistic safe sets are also calculated and shown in Fig: 9. There are three graphs for modes 1, 2 and 3. Each graph gives the probability of the temperatures in the rooms to be in the safe set for a specific initial condition. Any initial condition can be picked from the values of x-axis and y-axis and that point in the graph gives the maximal probability of being in the safe set.

5 Conclusions and future works

In this project we 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 of this model to other applications such as air traffic control.



(a) Sample paths of the temperatures for the execution corresponding to maximally safe policy

(b) Actions taken by the heater

Figure 10. Optimal probabilistic safe sets

Acknowledgments

My special gratitude to my mentors Saurabh Amin and Alessandro Abate, without them it cannot be done. I am gratefull to Professor Shankar Sastry to give me a clear view of CHESS and TRUST group. Thanks to the SUPERB and CHESS programs to select me for this research opportunity. Thanks to NSF for funding. I am thankful to my lab mates: Dominique Duncan(for always teasing me), Nashlie Sephus(for her calm appearance) and Heather Taylor(for her funny sounds). I had a great time in the lab with them and they helped me a lot in any difficulty. Thanks to all other SUPERB perticipants making my every day enjoyable in the International House. Thanks to my family and friends for all time support. Last but not the least very special thanks to Dr. Jonathan Sprinkle who was always present in need.

References

[1] An algorithmic introduction to numerical simulation of stochastic differential equations. *SIAM Review, 43(3)*, pages 525–546.

[2] S. Amin, J. Lygeros, S. Sastry, M. Prandini, and A. Abate. Reachability analysis for controlled discrete time stochastic hybrid systems. In J. Hespanha and A. Tiwari, editors, *Hybrid Systems: Computation and Control*, Lecture notes in Computer Science 3927, pages 49–63. Springer Verlag, 2006.

[3] J. Bect, Y. Phulpin, H. Baili, and G. Fleury. On the fokker-planck equation for stochastic hybrid systems: Application to a wind turbine model. *PMAPS*, 2006.

[4] A. Fehnker and F. Ivancic. Benchmarks for hybrid systems verification. *Hybrid Systems Computation and Control*, 2004.

[5] R. Malhame and C.-Y. Chong. Electric load model synthesis by diffusion approximation of a high-order hybrid-state stochastic system. *IEEE Transactions on Automatic Control AC-30(9)*, pages 854–860, 1985.

[6] C. J. Tomlin, J. Lygeros, and S. S. Sastry. A game theoretic approach to controller design for hybrid systems. *Proceedings of the IEEE*, pages 949–970, July 2000.