Safety of Stochastic Hybrid Systems Based on Discrete Approximations

Xenofon Koutsoukos Derek Riley

Abstract— **Stochastic hybrid system models can be used to analyze and design complex embedded systems that operate in the presence of uncertainty and variability. Verification of safety properties of such systems is a critical problem because of the interaction between the discrete and continuous stochastic dynamics. In this paper, we propose a probabilistic method for verifying safety based on discrete approximations. We show that the safety property can be characterized as a viscosity solution of a system of coupled Hamilton-Jacobi-Bellman equations. We present a computational algorithm for computing the solution based on discrete approximations and we show that this solution converges to the one for the original system as the discretization becomes finer. Finally, we illustrate the approach with a room heater example that has been proposed as a benchmark for hybrid system verification.**

I. Introduction

Many practical systems such as automobiles, chemical processes, and autonomous vehicles are best described by dynamics that comprise continuous state evolution within a mode of operation and discrete transitions from one mode to another, either controlled or autonomous. Such systems often interact with the environment in the presence of uncertainty and variability. Stochastic hybrid systems (SHS) can model such complex dynamics, uncertainty, multiple modes of operations, and they can support high-level control specifications that are required for design of autonomous or semi-autonomous applications.

Safety is the property that a system will not enter an unsafe state or configuration. Safety verification is a critical problem for complex embedded systems because of the interaction between the discrete and continuous stochastic dynamics. Safety specifications are usually expressed as formulas in appropriate logics. Given a specification formula encoding a safety property, the task is to determine whether the formal model of the system satisfies the property or generate a counterexample that violates the formula. In this paper, we proposed a probabilistic method for verifying safety. Instead of encoding the safety property with a logical formula that can be evaluated to be true or false, we consider a representation using measurable functions into [0,1] that characterizes what is the probability that the system will remain safe.

The contribution of the paper is twofold. First, we show that the measurable function that represents the probabilistic safety of a stochastic hybrid system can be characterized as a viscosity solution of a system of coupled Hamilton-Jacobi-Bellman equations. Second, we present a computational algorithm based on finite differences for computing the solution and we show that this solution converges to the one for the original system as the discretization becomes finer. Finally, we illustrate the approach with a room heater example that has been proposed as a benchmark for hybrid system verification.

In this paper, we consider the SHS model presented in [3]. A similar modeling framework and a simulation environment for concurrent stochastic hybrid systems is presented in [1]. Applications of stochastic hybrid systems include air traffic management systems [12] and communication networks [9]. Stochastic hybrid systems can be viewed as an extension of piecewise-deterministic processes [5] that incorporate stochastic continuous dynamics. Viscosity solution techniques in optimal control of piecewise deterministic processes have been investigated in [6]. Our approach generalizes these techniques to SHS based on results for continuous diffusions presented in [8].

This paper develops a systematic way to approximate stochastic hybrid systems that is amenable to computational methods [11]. The basic idea is to approximate the original processes by an appropriate Markov chain defined on a discrete state space. The approximation is achieved by constructing locally consistent chains that preserve local mean and covariance. Based on the discrete approximation, the verification problem can be solved using dynamic programming [13], [4]. The main advantage of this approach is that the analysis based on the discrete approximation is directly related to the original processes through the notion of local consistency, and further, it converges to the solution of the original problem. It should be noted that the same approach for optimal control of stochastic hybrid systems has been presented in [10].

The remaining of the paper is organized as follows. Section II formally describes the SHS model. Section III formulates the probabilistic safety problem. Section IV presents the discrete approximations based on finite differences. Section V outlines the computational algorithm and presents the convergence results. Section VI illustrates the approach for the room heater benchmark and Section VII concludes the paper.

II. Stochastic Hybrid Systems

We use the Stochastic Hybrid System (GSHS) model presented in [3]. Let Q be a set of discrete states. For each $q \in Q$, we consider the Euclidean space $\mathbb{R}^{d(q)}$ with dimension $d(q)$ and we define an invariant as an open set

This work was supported in part by NSF CAREER Award CNS-0347440.

Xenofon Koutsoukos and Derek Riley are with the EECS Department at Vanderbilt University, xenofon.koutsoukos,derek.riley@vanderbilt.edu.

$X^q \subseteq \mathbb{R}^{d(q)}$. The hybrid state space is denoted as $S = \bigcup_{q\in Q} q \times X^q$. Let $\bar{S} = S \cup \partial S$ and $\partial S = \bigcup_{q\in Q} q \times \partial X^q$ denote the completion and the boundary of S respectively. The Borel σ-field in S is denoted as $\mathcal{B}(S)$.

To define the execution of the system, we consider an $\mathbb{R}^p$-valued Wiener process and a sequence of *stopping times* $\{t_0 = 0, t_1, t_2, \ldots\}$ that represent the times when the continuous and discrete dynamics interact. Let the state at time t_i be $s(t_i) = (q(t_i), x(t_i))$ with $x(t_i) \in X^{q(t_i)}$. While the continuous state stays in $X^{q(t_i)}$, $x(t)$ evolves according to the stochastic differential equation (SDE)

$$dx = b(q, x)dt + \sigma(q, x)dw \tag{1}$$

where the discrete state $q(t) = q(t_i)$ remains constant and the solution of (1) is understood using the Itô stochastic integral.

The next stopping time is defined by $t^*_{i+1} = \inf\{t \geq t_i, x(t) \in \partial X^{q(t_i)}\}$. If $t_{i+1} = \infty$, the system continues to evolve according to (1) with $q(t) = q(t_i)$. If $t_{i+1} < \infty$, the system jumps at t_{i+1} to a new state $s(t_{i+1}) = (q(t_{i+1}), x(t_{i+1}))$ according to the transition measure $R(s(t^-_{i+1}, A))$ with $A \in \mathcal{B}(S)$. The evolution of the system is then governed by (1) with $q(t) = q(t_{i+1})$ until the next stopping time.

The following assumptions are imposed on the model. The functions $b(q, x)$ and $\sigma(q, x)$ are bounded and Lipschitz continuous in x for every q, and thus the SDE (1) has a unique solution. For the transition measure, it is assumed that $R(\cdot, A)$ is measurable for all $A \in \mathcal{B}(S)$ and $R(s, \cdot)$ is a probability measure for all $s \in \bar{S}$. Further, $R((q, x), dz)$ is assumed to be a stochastic continuous kernel.

Let $N_t = \sum_i I_{t\geq t_i}$ denote the number of jumps in the interval $[0, t]$. It is assumed that $E_s[N_t] < \infty$ for every initial state $s \in S$. Sufficient conditions for ensuring finitely many jumps can be formulated by imposing restrictions on the transition measure $R(s, A)$ [1].

In addition to the above assumptions, in this paper we assume that the set Q is finite and that X^q is bounded for every q. This is a reasonable assumption for many systems that have finitely many modes and saturation constraints on the continuous state. Even if the continuous state spaces are unbounded, often is desirable to approximate them for practical reasons. Further, we assume that the trajectories of the SHS satisfy a non-tangency condition with respect ∂X^q. A sufficient condition for the non-tangency assumption is that the the variance $\sigma(q, x)$ is non-degenerate (the diffusion matrix $a(q, x) = \sigma(q, x)\sigma^T(q, x)$ is positive definite). The non-tangency assumption can be satisfied even with degenerate variance by imposing appropriate conditions on the vector fields $b(q, x)$. In the remaining of the paper, we refer to the class of GSHS that satisfies the assumptions above simply as stochastic hybrid systems (SHS).

III. Probabilistic Safety

In this section, we formulate the safety problem for SHS. Let $T = \cup_{q\in Q_T}\{q\} \times T^q$ be a subset of S representing the set of safe states. The boundary of T is denoted by $\partial T = \cup_{q\in Q_T}\{q\} \times \partial T^q$. We assume that the set of unsafe states $X^q \setminus T^q$ for each q is a proper subset of X^q, i.e. $\partial X^q \cap \partial T^q = \emptyset$. The initial state (which, in general, is a probability distribution) must lie inside the safe set T and the transition measure $R(s, A)$ is defined so that the system cannot jump out of the safe set directly to the unsafe set. Consider the stopping time $\tau = \inf\{t \geq 0 : s(\tau^- \in \partial T)\}$. Let s be an initial state in T, then we define the function $V : \bar{T} \to \mathbb{R}$ by

$$V(s) = \begin{cases} E_s[I_{(s(\tau^-)\in\partial T)}], & s \in T \\ 1, & s \in \partial T \end{cases}.$$

The function $V(s)$ can be interpreted as the probability that a trajectory starting at s will reach the boundary ∂T of the safe set, i.e. the probability that the system is unsafe.

Inspired by [5], we add a new state Δ and we denote $T' = T \cup \Delta$. The system transitions to Δ according to the measure

$$R(s, \Delta) = \begin{cases} 1, & \text{if } s \in \partial T \\ 0, & \text{otherwise} \end{cases}.$$

The new process is indistinguishable from the original process $s(t)$ for $t < \tau$ and at time τ it jumps to Δ and stays there forever. The system dies immediately after transitioning to Δ, i.e. $b(\Delta) = \sigma(\Delta) = 0$. Finally, we extend V to T' by defining $V(\Delta) = 0$ which agrees with the probabilistic interpretation of V. By abuse of notation, we will denote the new process also by $s(t)$.

Next, we derive a representation of V that will be used to show that V is a viscosity solution. Given the safe set T, we construct a continuous bounded function $c : \bar{S} \to \mathbb{R}_+$ such that

$$c(q, x) = \begin{cases} 1, & \text{if } s \in \partial T^q \\ 0, & \text{if } s \in \partial X^q \end{cases}.$$

Then the value function V can be written as

$$V(s) = E_s\left[\int_0^\infty c(q_{t^-}, x_{t^-})dp^*(t)\right]$$

where $p^*(t) = \sum_{i=1}^\infty I_{(t\geq t_i)} I_{((q_{t_{i^-}}, x_{t_{i^-}})\in\partial S)}$ is a counting process counting the number of times the trajectory hits the boundary and jumps. The SHS satisfies the strong Markov property [3], and therefore, the Markov property can be applied not only for constant times but also for random stopping times. Let t_1 be the time of the first jump, then

$$V(s) = E_s\left[c(q_{t_1^-}, x_{t_1^-}) + \int_T V(y)R((q_t, x_t), dy)\right].$$

Let us define

$$\psi^V(q, x) = c(q, x) + \int_T V(y)R((q, x), dy)$$

then

$$V(s) = E_s[\psi^V(q_{t_1}, x_{t_1})]. \tag{2}$$

Assuming that the transition measure $R(s, A)$ is a continuous stochastic kernel, the map $(q, x) \to \int_\Gamma f(y)R((q, x), dy)$ is bounded uniformly continuous for every bounded and continuous function f [2]. Hence, if V is continuous, ψ^V will be continuous as well. Equation (2) is very similar to a cost criterion for a standard diffusion with a target set [11]. The

main difference is that the terminal cost $\psi^V(q,x)$ depends on the value function.

Consider the set of nonnegative Borel measurable functions $\mathcal{B}(S)_+$ and define the operator $\mathcal{G}: \mathcal{B}(S)_+ \to \mathcal{B}(S)_+$ by

$$Gg(q,x) = E_s[c(q_{t_1^-}, x_{t_1^-}) + g(q_{t_1}, x_{t_1})].$$

We will show that V is a fixed point of $\mathcal{G}$.

By the strong Markov property and the construction of the process [1]

$$E_s[c(q_{t_2^-}, x_{t_2^-}) + g(q_{t_2}, x_{t_2})|\mathcal{F}_{t_1}] =$$

$$E_s[c(q_{t_1}, x_{t_2^-}) + g(q_{t_2}, x_{t_2})|\mathcal{F}_{t_1}] = E_s[g(q_{t_1}, x_{t_1})].$$

Therefore,

$$\begin{aligned}\mathcal{G}^2 g(q,x) &= \mathcal{G}(\mathcal{G}g(q,x)) = E_s[c(q_{t_1^-}, x_{t_1^-}) + \mathcal{G}g(q_{t_1}, x_{t_1})] \\ &= E_s[c(q_{t_1^-}, x_{t_1^-}) + E_s[c(q_{t_2^-}, x_{t_2^-}) + g(q_{t_2}, x_{t_2})|\mathcal{F}_{t_1}]] \\ &= E_s[c(q_{t_1^-}, x_{t_1^-}) + c(q_{t_2^-}, x_{t_2^-}) + g(q_{t_2}, x_{t_2})].\end{aligned}$$

By induction, we get

$$\begin{aligned}G^n\psi(q,x) &= E_s[\sum_{i=1}^{n} c(q_{t_i^-}, x_{t_i^-}) + g(q_{t_n}, x_{t_n})] \\ &= E_s[\int_0^{t_n} c(q_{t^-}, x_{t^-}) dp^*(t) + g(q_{t_n}, x_{t_n})].\end{aligned}$$

Lemma 1 The value function $V(s)$ is a fixed point of the operator $\mathcal{G}$.

Proof By definition of $\mathcal{G}$, for any $g_1 \le g_2$ we have $\mathcal{G}g_1 \le \mathcal{G}g_2$. Let $v^0(q,x) = 0$ for every q and every x and set $v^{n+1}(q,x) = \mathcal{G}v^n(q,x)$. Then $\{v^n\}$ increases monotonically and further, v^n is finite for every n. Therefore, $\lim_{n\to\infty} v^n(q,x) = v(q,x)$ exists. Note that convergence is not guaranteed for other choices of v^0.

Since $v \ge v^n$, we have $\mathcal{G}v \ge \mathcal{G}v^n$ and thus $\mathcal{G}v \ge v^{n+1}$ for all n, therefore $\mathcal{G}v \ge v$. In addition, $\mathcal{G}v^n = v^{n+1} \le v \le \mathcal{G}v$ and $\lim_{n\to\infty} v^n = v$, therefore $\mathcal{G}v \le v \le Gv$ and $v = \lim_{n\to\infty} v^n$ is a fixed point of $\mathcal{G}$.

Finally, $v = \lim_{n\to\infty} G^n v^0 = E_s[\int_0^\infty c(q_{t^-}, x_{t^-}) dp^*(t)]$ therefore V is a fixed point of $\mathcal{G}$, i.e. $V(s) = \mathcal{G}V(s)$.

Lemma 2 V is bounded and piecewise continuous in $\bar{T}$.

Proof Boundness is straightforward from the definitions. Since $R(s,A)$ is a continuous stochastic kernel, the map $(q,x) \to \int_T f(y)R((q,x),dy)$ is bounded uniformly continuous for every bounded and continuous function f [2]. Assuming nondegeneracy of the variance $\sigma(q,x)$, the stopping time t_1 depends continuously on the sample paths starting at $x(t_0)$ [11] and by the strong Markov property this is true for every t_i. Therefore, $V(s)$ is continuous on $\bar{T}^q$ for each q.

Theorem 1 Assume that f and σ are continuously differentiable in $\bar{T}^q$ for each q and for suitable C_1 and C_2 satisfy $|f_x| \le C_1$, $|\sigma_x| \le C_1$, and $|f(q,0)| + |\sigma(q,x)| \le C_2$. Then V is the unique viscosity solution of

$$\mathcal{H}(q,x,D_xV,Dx^2V) = 0 \text{ in } T^q,\ q \in Q \tag{3}$$

with boundary condition

$$V(q,x) = \psi^V(q,x) \text{ on } \partial T^q,\ q \in Q \tag{4}$$

where

$$\mathcal{H}(q,x,D_xV,D_x^2V) = f(q,x)D_xV + \frac{1}{2}\text{tr}(\sigma(q,x)\sigma^T(q,x)D_x^2V).$$

Proof First, we claim that

$$v(q,x) = \begin{cases} \mathcal{G}g(q,x) & \text{in } T^q,\ q \in Q \\ \psi^g(q,x) & \text{on } \partial T^q,\ q \in Q \end{cases}$$

is bounded and continuous in $\bar{T}^q$ and it is a unique viscosity solution of

$$\mathcal{H}(q,x,D_xV,Dx^2V) = 0 \quad \text{in} \quad T^q,\ q \in Q \tag{5}$$

$$V(q,x) = \psi^g(q,x) \quad \text{on} \quad \partial T^q,\ q \in Q. \tag{6}$$

For each q, this is the HJB equation of the exit problem of an ordinary diffusion described by the SDE (1). Further, $\psi^g(q,x)$ is bounded uniformly continuous and we can apply the results of [8] (Thm V.2.1 and Cor. V.3.1) to verify the claim. From Lemma 1 and Lemma 2, we know that V is a fixed point of $\mathcal{G}$ and that is bounded and continuous. Further, $\psi^V(q,x)$ is bounded uniformly continuous and by applying again the results of [8], we conclude that V is the unique viscosity solution of (3)-(4).

IV. Discrete Approximations

In this paper, we develop computational methods for safety verification of stochastic hybrid systems based on discrete approximations. This section employs the approximation method presented in [11] for computing locally consistent Markov chains (MCs). The local mean and covariance for the SDE (1) on the interval $[0,\delta]$ are

$$\begin{aligned}E[x(\delta) - x] &= b(q(t),x(t))\delta + o(\delta) \\ E[(x(\delta) - x)(x(\delta) - x)^T] &= a(q(t),x(t))\delta + o(\delta).\end{aligned}$$

where $a(q,x) = \sigma(q,x)\sigma^T(q,x)$. Let $\{\xi_n\}$ be an MC on a discrete state space $S_q^h \subset X^q$ with transition probabilities denoted by $p((q,x),(q,y))$. A locally consistent MDP must satisfy

$$E[\Delta\xi_n^h] = b(q,x)\Delta t^h(q,x) + o(\Delta t^h(q,x))$$

$$\begin{aligned}E[(\Delta\xi_n^h - E[\Delta\xi_n^h])(\Delta\xi_n^h - E[\Delta\xi_n^h])^T] &= \\ \sigma(q,x)\sigma^T(q,x)\Delta t^h(q,x) &+ o(\Delta t^h(q,x))\end{aligned}$$

where $\Delta\xi_n^h = \xi_{n+1}^h - \xi_n^h, \xi_n^h = x$ and $\Delta t^h(q,x)$ are appropriate interpolation intervals (or the "holding times") for the MC.

The transition probabilities $p^h((q,x),(q,y))$ and the interpolation intervals can be computed systematically from the parameters of the SDE (details can be found in [11]). In the case the diffusion matrix $a(q,x)$ is diagonal and we consider a uniform grid with e_i denoting the unit vector in the i^{th} direction, the transition probabilities are

$$p^h((q,x),(q,x \pm he_i)) = \frac{a_{ii}(q,x)/2 + hb_i^{\pm}(q,x)}{Q(q,x)} \tag{7}$$

[1] $\mathcal{F}_t$ denotes the filtration of the SHS process.

and the interpolation interval is

$$\Delta t^h(q,x) = \frac{h^2}{Q^h(q,x)} \tag{8}$$

where $Q^h(q,x) = \sum_i [a_{ii}(q,x) + h|b_i(q,x)|]$ and $a^+ = \max\{a,0\}$ and $a^- = \max\{-a,0\}$.

Equation (7) gives the transition probabilities for all the interior (discrete) points of S_h^q. The stochastic hybrid system can be approximated by "discretizing" the boundaries and approximating the transition measure $R(s,A)$ by a discrete transition probability kernel. Details are omitted due to length limitations. Finally, all the boundary points of the safe set are assumed to be absorbing.

V. Computational Algorithms and Convergence

Consider the approximating MDP $\{s_n^h\} = \{\xi_n^h, q_n^h\}$ with transition probabilities $p^h((q,x),(q,y))$ defined in Section IV and denote ν_h the stopping time representing that $(q_n^h, \xi_n^h\}$ reaches ∂T. Then, the value function V of can be approximated by

$$V^h(s) = E_s\left[c(q_{\nu_h}^h, \xi_{\nu_h}^h)\right].$$

Since the approximating process is discrete, the above equation can be written as

$$V^h(q,x)) = \left[\sum_{y,q'} p^h((q,x,(q,y)V^h(q',y)\right]$$

if x is and interior point and $V^h(q,x) = c(q,x)$ on the boundary of the safe set.

$V^h(q,x)$ can be computed using a value iteration algorithm. To show the convergence of the algorithm, first we transform the problem to an equivalent problem by adding a terminal state Δ similar to Section III. Consider an MC with state space $\tilde{S}^h = S^h \cup \{\Delta\}$ and define the transition probabilities so that $\tilde{p}^h((q,x),\Delta) = 1$, if; $x \in S_h^q$, $\tilde{p}^h(\Delta,\Delta) = 1$, and $\tilde{p}^h((q,x),(q',x')) = p^h((q,x),(q',x'))$ otherwise. This means the when the MC hits the boundary of the safe set, it transitions to the state Δ and stays there for ever. Consider the function $\tilde{c} : \tilde{S} \to \mathbb{R}_+$ with $\tilde{c}(\Delta) = 1$ and $\tilde{c}(q,x) = 0$ for every q and x. By abuse of notation, we will denote the new process also by $\{s_n\}$. Consider the value function

$$\tilde{V}(s) = E_s[\sum_{t=0}^{\infty} \tilde{c}(s(t))]. \tag{9}$$

Clearly, this sum is well defined and bounded and $\tilde{V} = V$.

Proposition 1 Let $\tilde{V}_0^h(q,x) = 0$, then the iteration

$$\tilde{V}_{n+1}^h(q,x) = \left[\sum_{y,q'} p^h((q,x,(q,y)\tilde{V}^h(q',y)\right] \tag{10}$$

with $\tilde{V}(\Delta) = 1$ converges to $\tilde{V}^h = V^h$.

Proof Consider the value function described by (9) for $\{s_n^h\}$. Computing $\tilde{V}^h$ is a special case of the total expected reward criterion for positive models [13]. The iteration (10) may have multiple fixed points but if we pick $\tilde{V}_0^h(q,x) = 0$ the iteration converges to the least fixed point $\tilde{V}^h$ [13] (Thm 7.2.12).

Finally, we show that the value function $V^h(q,x)$ obtained based on the approximating MC converges to the value function of the SHS as $h \to 0$.

Theorem 2 Let $V^h(q,x)$ be a solution of

$$V^h(q,x)) = \left[\sum_{y,q'} p^h((q,x,(q,y)V^h(q',y)\right] \tag{11}$$

with boundary condition $V^h(q,x) = c(q,x), x \in \partial T$. Then

$$\lim_{y \to x, h \to 0} V^h(q,y) = V^h(q,x).$$

Proof Let $g \in \mathcal{B}(S)_+$ be a continuous and bounded function and suppose that V is the unique viscosity solution of (5-6) that is bounded and continuous in $\bar{T}^q$. Consider $\bar{\Sigma}_q^h$ to be a discretization of $\bar{T}^q$ and denote Σ_q^h and $\partial\Sigma_q^h$ the set of interior and boundary points respectively. Using the approximation described in Section V the dynamic programming equation for $\bar{\Sigma}_q^h$ can be written as

$$V^h(q,x) = \begin{cases} F^h[V^h(\cdot)](q,x) & \text{if } x \in \Sigma_q^h \\ \psi^g(q,x) & \text{if } x \in \partial\Sigma_q^h \end{cases}.$$

V is continuous and bounded viscosity solution of (5-6) and $\psi^g(q,x)$ is continuous. Therefore, for each q we have a standard exit problem from T^q for the SDE (1) and by applying the results of [8] (Sec. IX.5) we have that V^h converges uniformly to V.

To show convergence of V^h for the SHS, we replace g by V and we follow an argument similar to the proof of Thm 1. Assume that V is given and define

$$\bar{V}^h(q,x) = \begin{cases} F^h[\bar{V}^h(\cdot)](q,x) & \text{if } x \in \Sigma_q^h \\ \psi^V(q,x) & \text{if } x \in \partial\Sigma_q^h \end{cases}.$$

Since V is bounded and continuous we have $\lim_{y \to x, h \to 0} \bar{V}^h(q,y) = \bar{V}(q,x)$. Assume that for each h, $\bar{V}^h$ is computed by a value iteration algorithm with $v^0 = 0$. Then, V^h is a fixed point of F_V^h and therefore, $\bar{V}^h = V^h$ for every h and $\bar{V} = V$. Therefore, $\lim_{y \to x, h \to 0} V^h(q,y) = V(q,x)$.

VI. Room Heater Benchmark

A modeling benchmark of a room heating problem has been presented in [7]. The benchmark models the temperature dynamics of a building with three rooms and two mobile heaters. The temperature in each room x_i depends on the temperature of the adjacent rooms, the outside temperature u, and whether a heater is in the room.

The SDE describing the continuous dynamics of the system is

$$dx = (Ax + Bu + Cq)\,dt + \Sigma dw$$

where

$$A = \begin{bmatrix} -.9 & .5 & 0 \\ .5 & -1.3 & .5 \\ 0 & .5 & -.9 \end{bmatrix},\ B = \begin{bmatrix} .4 \\ .3 \\ .4 \end{bmatrix},$$

$C = diag(6, 7, 8)$, $u = 4$, $\Sigma = diag(0.1)$, and $w(t)$ is an $\mathbb{R}^3$-valued Wiener process.

The discrete states of the system describe the position and condition of the heaters in the rooms. If a heater is in a room and on, then a one is placed in the corresponding position of that room. If the heater is not in the room or is in the room but off, then a zero is placed in the corresponding position. The heating benchmark has twelve heater modes as shown in Figure 1. Mode transitions are denoted by the arcs between nodes and are defined using a control policy for moving the heater. The control policy is encoded by labeling the transitions using guard conditions to encode the control policy. Consider rooms i and j. If a heater is present in room i, but off, it is switched on if $x_i \leq on_i$ and a heater that is on is switched off if $x_i \geq off_i$. A heater is moved from room j to an adjacent room i if the following conditions are true: (i) room i is without a heater, (ii) room j currently has a heater, (iii) $x_i \leq get_i$, and (iv) $x_j - x_i \geq dif_i$.

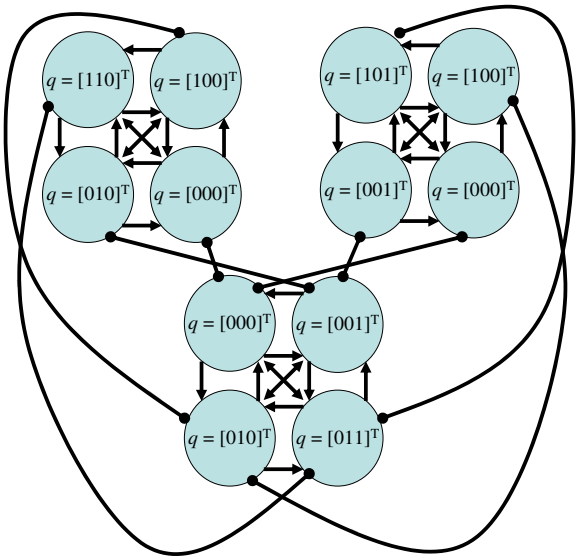

Fig. 1. Automaton

We discretized the continuous state space by assuming that the safe set is described by $x_i = [10, 20], i = 1, 2, 3$ and the approximation parameter was set to $h = 0.25$. The room heater benchmark evolves in a three-dimensional continuous state space, hence it is difficult to visualize the value function. To illustrate our results, we have set a pre-defined threshold (0.1) that describes the acceptable probability for reaching the unsafe set. Then, for each initial mode we plot the "safe" set as the set of states that have a probability below the threshold to reach the unsafe set. Figure 2 shows the the safe set. The iterative algorithm executed in approximately 49 minutes on a 3.0 GHz desktop computer.

VII. Conclusions and Future Work

This paper employs an approximation method for solving the safety problem for stochastic hybrid systems. The main advantage of the method is that it guarantees the convergence of the solution based on the discrete approximation to the solution of the original problem. The approach gives rise to several significant problems. A fundamental challenge is to develop scalable numerical methods that can be applied to large systems. Towards this goal, currently we are investigating methods based on variable resolution grids, parallel methods, and as methods based on value function approximation.

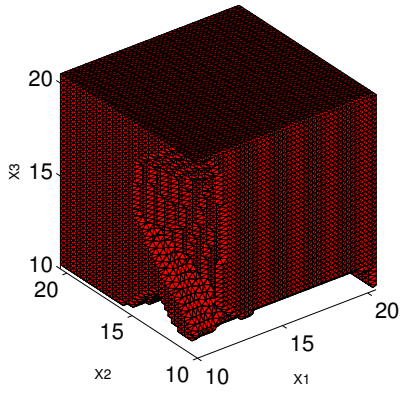

Fig. 2. Room heater benchmark safe states for $q = [110]^T$

References

[1] M. Bernadskiy, R. Sharykin, and R. Alur Structured Modeling of Concurrent Stochastic Hybrid Systems. *Joint Conference on Formal Modelling and Analysis of Timed Systems and Formal Techniques in Real-Time and Fault Tolerant Systems*. Grenoble, France, September 2004.

[2] D.P. Bertsekas and S.E. Shreve *Stochastic Optimal Control: The Discrete Time Case*. Academic Press, 1978.

[3] M. Bujorianu, J. Lygeros, "Theoretical Foundations of General Stochastic Hybrid Systems: Modeling and Optimal Control", *In Proceedings of 43rd IEEE Conference on Decision and Control*, 2004.

[4] C. Courcoubetis and M. Yannakakis, "The complexity of probabilistic verification", *Journal of ACM*, 42(4), pp, 857-907, 1995.

[5] M. Davis, *Markov Models and Optimization*, Chapman and Hall, 1993.

[6] M. Davis and M. Farid, Piecewise-deterministic processes and viscosity solutions, In *Stochastic Analysis, Control, Optimization and Applications: A Volume in Honor of W.H. Fleming*, pp. 249-268, Birkhauser, 1999.

[7] A. Fehnker and F. Ivancic, "Benchmarks for Hybrid Systems Verification", *Hybrid Systems: Computation and Control - HSCC 2004*, LNCS 2993, pp. 326-341, Springer, 2004.

[8] W. Fleming, H. Soner, *Controlled Markov Processes and Viscosity Solutions*, Springer-Verlag, 1993.

[9] J.P. Hespanha. Stochastic Hybrid Systems: Application to Communication Networks. In *Hybrid Systems: Computation and Control - HSCC 2004*, LNCS 2993, pp. 387-401, Springer, 2004.

[10] X. Koutsoukos, "Optimal Control of Stochastic Hybrid Systems Based on Locally Consistent Markov Decision Processes", *International Journal of Hybrid Systems*, 4, 301-318, 2004.

[11] H.J. Kushner and P. Dupuis. *Numerical Methods for Stochastic Control Problems in Continuous Time*. Springer, 2001.

[12] G. Pola, M. Bujorianu, J. Lygeros, and M. Di Benedetto. Stochastic Hybrid Models: An Overview with Application to Air Traffic Management. In *IFAC ADHS03*, June 2003.

[13] M. Puterman, *Markov Decision Processes-Discrete Stochastic Dynamic Programming*, Wiley: Hoboken, New Jersey, 2005.