Computational Methods for Verification of Stochastic Hybrid Systems

Xenofon D. Koutsoukos, *Senior Member, IEEE*, and Derek Riley

***Abstract*—Stochastic hybrid system (SHS) models can be used to analyze and design complex embedded systems that operate in the presence of uncertainty and variability. Verification of reachability properties for such systems is a critical problem. Developing sound computational methods for verification is challenging because of the interaction between the discrete and the continuous stochastic dynamics. In this paper, we propose a probabilistic method for verification of SHSs based on discrete approximations focusing on reachability and safety problems. We show that reachability and safety can be characterized as a viscosity solution of a system of coupled Hamilton–Jacobi–Bellman equations. We present a numerical algorithm for computing the solution based on discrete approximations that are derived using finite-difference methods. An advantage of the method is that the solution converges to the one for the original system as the discretization becomes finer. We also prove that the algorithm is polynomial in the number of states of the discrete approximation. Finally, we illustrate the approach with two benchmarks: a navigation and a room heater example, which have been proposed for hybrid system verification.**

***Index Terms*—Reachability analysis, stochastic hybrid systems (SHSs), verification.**

I. Introduction

STOCHASTIC hybrid system (SHS) models can be used to analyze and design complex embedded systems that operate in the presence of uncertainty and variability since they incorporate complex dynamics, uncertainty, and multiple modes of operations and they can support high-level control specifications that are required for the design of autonomous or semiautonomous applications. Verification of the reachability properties for such systems aims at determining the probability that the system will reach a set of desirable or unsafe states, and it is a critical problem because of the interaction between the discrete and the continuous stochastic dynamics.

Reachability and safety properties for (nonstochastic) hybrid systems are usually expressed as formulas in appropriate logics. Given a specification formula encoding a property, the task is to determine whether the formal model of the system satisfies the property or to generate a counterexample that violates the formula. In this paper, we propose a probabilistic method for verification of reachability properties. Instead of encoding the reachability property with a logical formula that can be evaluated to be true or false, we consider a representation using measurable functions taking values in [0, 1] that characterize the probability that the system satisfies the property. Such a real-valued logic framework is based on the seminal work by Kozen [1], which generalizes logic to handle probabilistic phenomena. An approach for the analysis of probabilistic systems based on similar logics and discounting of the future has been presented in [2].

This paper addresses verification for the reachability and safety problems for SHSs. The main contribution is the characterization of reachability and safety properties as viscosity solutions of a system of coupled Hamilton–Jacobi–Bellman (HJB) equations. Based on this formulation, this paper proposes a computational method based on discrete approximations for solving reachability analysis problems for SHSs.

Specifically, we show that reachability for SHSs can be represented by a measurable function that is interpreted as the probability that an arbitrary initial state will reach a target set while avoiding an unsafe set. This paper shows that this function is a value function of a dynamic programming problem and can be characterized as a fixed point of a recursive operator defined with respect to the (random) stopping times that represent the times of the discrete jumps. Assuming nondegeneracy for the diffusion term of the stochastic continuous dynamics, we show that the value function is bounded and continuous. These properties are then used to prove that the value function for the reachability problem of SHSs is similar to the value function for the exit problem of a standard stochastic diffusion, but the running and terminal costs depend on the value function itself. Based on this formulation, we show the main result of this paper, which characterizes the value function as a viscosity solution of a system of coupled HJB equations.

One of the advantages of characterizing reachability properties using viscosity solutions is that for computational purposes we can employ numerical algorithms based on discrete approximations. We use an approximation method for SHSs based on finite-differences similar to the methods presented in [3]. We present an iterative algorithm based on dynamic programming for computing the solution and we show that the algorithm converges for appropriate initial conditions. Furthermore, we show that the solution based on the discrete approximation converges to the one for the original SHS as the discretization becomes finer. The proof of the convergence is a straightforward extension to the SHSs of the results presented in [4]. Regarding the efficiency of the computational methods, we prove that the

Manuscript received March 13, 2006; revised November 1, 2006. This work was supported in part by the National Science Foundation under NSF Career Award CNS-0347440. This paper was recommended by Associate Editor G. C. Calafiore.

The authors are with the Institute for Software Integrated Systems, Department of Electrical Engineering and Computer Science, Vanderbilt University, Nashville, TN 37235 USA (e-mail: Xenofon.Koutsoukos@vanderbilt.edu; Derek.Riley@vanderbilt.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSMCA.2007.914777

iterative algorithm is polynomial in the number of states of the discrete approximation process. This number exponentially grows with the dimension of the continuous state space, and therefore, scalability to high-dimensional systems is a limiting factor of the approach. Finally, we illustrate our results with a navigation benchmark and a room heater benchmark that have been proposed for hybrid system verification [5]. Preliminary results of our approach have been presented in [6].

The rest of this paper is organized as follows. Section II compares the proposed approach with existing work on SHSs and computational methods for verification of hybrid systems. Section III describes the SHS model. Section IV formulates the reachability and safety problem and characterizes their solution. Section V presents and analyzes the numerical methods based on discrete approximations. Section VI illustrates the approach using two benchmarks, and Section VII concludes this paper.

II. Related Work

In this paper, we adopt the model presented in [7], which can be viewed as an extension of the SHSs described in [8]. An important characteristic of this model used in our analysis is that it satisfies the strong Markov property [7]. Related models have been presented in [9], with emphasis on the modeling and analysis of communication networks, and in [10] for the simulation of concurrent systems. A technique for probabilistic verification for discrete-time SHSs based on an optimal control formulation has been presented in [11]. Mathematical tools for analyzing the reachability of SHSs based on the theory on Dirichlet forms that implies the development of computational methods based on theorem provers have been presented in [12]. A method for safety verification based on overapproximation of the safe set using barrier certificates has been developed in [13].

SHSs can be viewed as an extension of piecewise deterministic processes [14] that incorporate stochastic continuous dynamics. Reachability of such systems has been studied in [15]. Communicating piecewise Markov processes have been presented in [16] with emphasis on concurrence. Optimal control of piecewise deterministic processes has been studied in [17], where it is proven that the value function is the unique viscosity solution of a first-order HJB equation. The work in [17] is based on a dynamic programming argument for characterizing the value function as a fixed point of an appropriate recursive operator and considers a discounted optimal control criterion that ensures that the recursive operator is contractive in order to prove convergence. In contrast, our work considers a reachability criterion for SHSs for which the value function is a viscosity solution of a set of coupled second-order HJB equations. The results of [17] cannot be applied, because the presence of stochastic continuous dynamics and the absence of a discount factor in the reachability criterion require new techniques for proving convergence.

Reachability properties for continuous and hybrid systems have been characterized as viscosity solutions of variants of HJB equations in [18] and [19]. Extensions of this approach to SHSs and a toolbox based on level set methods have been presented in [20]. Level set methods are also based on a discretization of the state space, but they may offer computational advantages since the computation is limited to a neighborhood of the reachable set. The dynamic programming approach described in this paper is usually simpler to implement and capture the dependence of the value function between discrete modes. The approach also allows us to show the convergence of the solution obtained using the numerical methods to the solution of the SHS.

Discrete approximation methods based on finite differences have been studied extensively in [3] and the references therein. Convergence results justifying the use of discrete approximation techniques for stochastic optimal control problems have been presented in [3] and [4]. Based on discrete approximations, the reachability problem can be solved using algorithms for discrete processes [21]–[23]. The approach has been applied for optimal control of SHSs, given the discounted cost criterion in [24]. For verification of reachability properties, the discount term cannot be used, and convergence of the value function can be ensured only for appropriate initial conditions. A related grid-based method for safety analysis of stochastic systems with applications to air traffic management has been presented in [25]. Our approach is similar, but using viscosity solutions, we show the convergence of the discrete approximation methods.

This section also compares the proposed approach with existing computational methods for (nonstochastic) hybrid systems. To our knowledge, computational methods for verification of SHSs have not been reported in the literature. Hybrid systems can be verified by two types of techniques: 1) *overapproximative* and 2) *convergent* [26].

In overapproximative verification techniques, each step of the verification algorithm is designed to produce an overapproximation of the forward or backward reachable set. These methods use set representations such as polyhedra or ellipsoids and have been reported to scale well up to about six dimensions for general hybrid systems. If the reachable set is not initially found to be safe, it is required to tighten the verification variables and approximations. Therefore, multiple attempts may be necessary to verify a system, and it cannot be guaranteed that a solution can always be found.

The *d/dt* tool uses an overapproximation based on convex sets using griddy polyhedra expressed as closed-unit hypercubes with integer vertices [27]. Polyhedral approximations of flow pipes are used to calculate the forward reachable sets from an initial polyhedral set for linear dynamics. *CheckMate* is a Matlab-based tool that has similar requirements and uses a similar verification algorithm as *d/dt* [28]. *VeriSHIFT* is a tool that employs ellipsoidal sets and time-varying linear dynamics to calculate the reachable set using a similar technique as *d/dt* [29]. The *predicate abstraction* technique reported in [30] requires the specification of appropriate predicates that divide the state space into a finite number of regions. Continuous and discrete successors are calculated similarly to *d/dt*, but the predicate abstraction technique only calculates the intersection of the successors with other abstract states instead of the union with previous reachable states such as *d/dt*, *CheckMate*, or *VeriSHIFT* [30].

Performance results have been reported in [5] for the navigation benchmark (see Section VI) using *d/dt* and the predicate

abstraction method. Because the performance of the verification using either technique varies with the choice of initial state, several initial states were tested. While some tests completed in just seconds, others were unable to return a solution. Some of the problems that *d/dt* could not verify were verified using predicate abstraction inasmuch as 78 min on an instance of the navigation benchmark with nine discrete states. These tests were executed on a four-processor Sun Enterprise 3000 with 4 GB of memory.

It is difficult to compare these results with our approach, because the performance of our algorithm is not dependent on a set of initial states. Furthermore, our technique will verify SHSs with nonlinear continuous dynamics. Our method is able to generate reachability results for every state of a 25-location version of the navigation benchmark at a resolution of 0.1 in under 200 min on a 2-GHz desktop computer with 1 GB of memory.

Convergent approximative techniques solve the verification problem by approximating the hybrid system with another model of computation for which there exist well-understood verification methods. These techniques generally use grids to discretize the state space and allow the user to choose the resolution of the approximation. Examples of this technique include the level set method (LSM) [19] and our approximation using locally consistent discrete Markov processes.

The LSM is based on two-person zero-sum game theory to determine an implicit representation of the boundary of the reachable set. Performance results are not as good as those of overapproximative methods, but the LSM has been used on systems with five dimensions [26]. One benefit of convergent techniques is that they generally do not restrict the dynamics of the system or the shape of the reachable set. We have verified a stochastic version of the collision avoidance problem described in [26] with our method and found that our method has a similar performance as the LSM. One of the advantages of our method is that it can be easily parallelized. In our preliminary work on parallel methods for verification of SHSs, we have been able to verify 7-D systems [31] by applying known decomposition methods from parallel dynamic programming [32].

III. SHSs

We adopt the general SHS (GSHS) model presented in [7]. This section describes the model and establishes the notation.

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 $X^q \subseteq \mathbb{R}^{d(q)}$. 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 $\mathcal{B}(S)$.

Definition 1: A GSHS is defined as $H = ((Q, d, \mathcal{X}), b, \sigma, Init, \lambda, R)$, where

- Q is a set of discrete states (modes);
- d: $Q \to \mathbb{N}$ is a map that defines the continuous state space dimension for each $q \in Q$;
- $\mathcal{X}$: $Q \to \mathbb{R}^{d(\cdot)}$ is a map that describes the invariant for each $q \in Q$ as an open set $X^q \subseteq \mathbb{R}^{d(q)}$;
- b: $Q \times X^q \to \mathbb{R}^{d(q)}$ and σ: $Q \times X^q \to \mathbb{R}^{d(q)\times p}$ are drift vectors and dispersion matrices, respectively;
- $Init$: $\mathcal{B}(S) \to [0, 1]$ is an initial probability measure on S;
- λ: $\bar{S} \to \mathbb{R}_+$ is a nonnegative transition rate function;
- R: $\bar{S} \times \mathcal{B}(\bar{S}) \to [0, 1]$ is a transition measure.

To define the execution of the system, we denote the underlying probability space as $(\Omega, \mathcal{F}, P)$ and consider an $\mathbb{R}^p$-valued Wiener process $w(t)$ and a sequence of *stopping times* $\{t_0 = 0, t_1, t_2, \ldots\}$. Let the state at time t_i be $s(t_i) = (q(t_i), x(t_i))$[1] 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), i.e.,

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

where the discrete state $q(t) = q(t_i)$ remains constant and the solution of (1) is understood using the Itô stochastic integral [33]. A sample path of the stochastic process is denoted by $x_t(\omega)$, $t > t_i$, and $\omega \in \Omega$.

The next stopping time t_{i+1} represents the time when the system transitions to a new discrete state. The discrete transition occurs either because the continuous state x exits the invariant $X^{q(t_i)}$ of the discrete state $q(t_i)$ or based on an exponential distribution with transition rate function λ. Therefore, t_{i+1} can be defined as the minimum between two other stopping times: 1) the first hitting time of the boundary $\partial X^{q(t_i)}$ defined as $t^*_{i+1} = \inf\{t \geq t_i, x(t) \in \partial X^{q(t_i)}\}$ and 2) a stopping time τ_{i+1} described by an exponential distribution with survivor function, i.e.,

$$M(t, \omega) = \exp\left(-\int_{t_i}^{t} \lambda\left(q(t_i), x_z(\omega)\right) dz,\right), \quad \omega \in \Omega.$$

Thus, the time of the next discrete transition t_{i+1} is a stopping time whose distribution is defined by the survivor function

$$F(t, \omega) = I_{(t<t^*_{i+1})} \exp\left(-\int_{t_i}^{t} \lambda\left(q(t_i), x_z(\omega)\right) dz\right)$$

where I denotes the indicator function.[2]

At time t_{i+1}, the system will transition to a new discrete state, and the continuous state may jump according to reset measure R. The trajectory of $x(t)$ is assumed to be left-continuous, so we denote the solution of (1) at $t = t_{i+1}$ as $x(t^-_{i+1})$ and $s(t^-_{i+1}) = (q(t^-_{i+1}), x(t^-_{i+1}))$, where $q(t^-_{i+1}) = q(t_i)$ is the discrete state before the transition. 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 transition measure $R(s(t^-_{i+1}), A)$, with $A \in \mathcal{B}(S)$. The evolution of the system is then governed by the SDE (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

[1]When there is no confusion, we will interchangeably use the notation (q, x) and s for the hybrid state to simplify complex formulas, and often, we will use the notation $s_{t_i} = (q_{t_i}, x_{t_i})$ for brevity.

[2]Given a set $A \in \mathcal{F}$, the indicator function is defined as $I_A(\omega) = 1$ if $\omega \in A$ and 0 if $\omega \notin A$.

continuous in x for every q; thus, SDE (1) has a unique solution. The transition rate function λ is a bounded and measurable function that is assumed to be integrable for every $x_t(\omega)$. For the transition measure, it is assumed that $R(\cdot, A)$ is measurable for all $A \in \mathcal{B}(S)$, $R(s, \cdot)$ is a probability measure for all $s \in \bar{S}$, and $R((q,x), dz)$ is a stochastic continuous kernel.

Let $N_t = \sum_i I_{t \geq t_i}$ denote the number of jumps in interval $[0,t]$. It is assumed that the expected number of jumps is finite for every initial state $s \in S$, i.e., $E_s[N_t] < \infty$. A sufficient condition for ensuring finitely many jumps can be formulated by imposing restrictions on the transition measure $R(s,A)$. Let $s = (q,x)$ be the state after a discrete transition. If, for every $x \in A$, $d(x, \partial X^q) \geq \epsilon > 0$[3] and $\exists \delta > 0$ such that $P[\inf\{t > t_{i+1}, x(t) \in \partial X^q\} \geq \delta] = 1$, then $t_{i+1} - t_i > \delta$, $i = 1, 2, \ldots$, with a probability of 1. This condition is satisfied if the continuous state after a jump is in the interior of an invariant.

Additionally, in this paper, we consider the two following assumptions:

Assumption 1—Nondegeneracy: The boundaries ∂X^q are assumed to be sufficiently smooth, and the trajectories of the system satisfy a nontangency condition with respect to the boundaries. A sufficient condition for the nontangency assumption is that the diffusion term is nondegenerate, i.e., $a(q,x) = \sigma(q,x)\sigma^T(q,x)$ is positive definite. This assumption is used to show the continuity of the viscosity solution close to the boundaries [4]. It should be noted that it is possible to show the continuity of the viscosity solution close to the boundaries even with degenerate variance by imposing appropriate conditions [3], [4].

Assumption 2—Boundness: It is assumed 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 state space is unbounded, it is often desirable to approximate it for applying numerical methods. By defining appropriately the boundary conditions, it can be shown that the effect of the numerical cutoff is small [4]. This assumption is used for approximating the hybrid system by a finite Markov chain (MC) and employing numerical methods based on dynamic programming.

In the remainder of this paper, we refer to the class of GSHS that satisfies the preceding assumptions as SHSs.

IV. Probabilistic Verification

In this section, we formulate the reachability problem for SHS, and we show that reachability can be characterized as a viscosity solution of a system of coupled HJB equations.

A. Reachability

Given a target set and an unsafe set of states, the objective of the reachability problem is to compute the probability that the system execution from an arbitrary initial state will reach the target set while avoiding the unsafe set.

[3] $d(x, \partial X^q)$ denotes the Euclidean distance between x and ∂X^q.

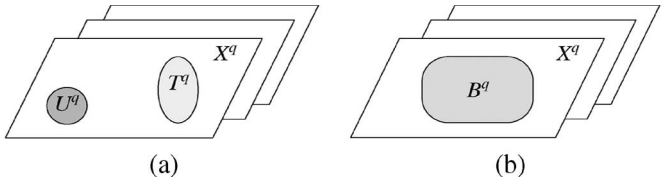

Fig. 1. (a) Reachability and (b) safety.

In general, the target and unsafe sets for SHS may be described as unions of target and unsafe sets, respectively for multiple modes. For example, a target set may be independent of the discrete state and represented as a subset of the continuous state space, which requires considering a target subset for every discrete state. Let $T = \cup_{q \in Q_T}\{q\} \times T^q$ and $U = \cup_{q \in Q_U}\{q\} \times U^q$ be subsets of S representing the set of target and unsafe states, respectively. The reachability problem is illustrated in Fig. 1(a). We assume that T^q and U^q are proper open subsets of X^q for each q, i.e., $\partial T^q \cap \partial X^q = \partial U^q \cap \partial X^q = \emptyset$ and the boundaries ∂T^q and ∂U^q are sufficiently smooth. We define $\Gamma^q = X^q \setminus (\bar{T}^q \cup \bar{U}^q)$ and $\Gamma = \cup_{q \in Q}\{q\} \times \Gamma^q$. The initial state (which, in general, is a probability distribution) must lie outside sets T and U. Transition measure $R(s,A)$ is assumed to be defined so that the system cannot jump directly to U or T.

Consider the stopping time $\tau = \inf\{t \geq 0 : s(t) \in \partial T \cup \partial U\}$ corresponding to the first hitting time of the boundary of the target or unsafe set. Let s be an initial state in Γ; then, we define the function $V : \bar{\Gamma} \to \mathbb{R}_+$ as

$$V(s) = \begin{cases} E_s\left[I_{(s(\tau^-) \in \partial T)}\right], & s \in \Gamma \\ 1, & s \in \partial T \\ 0, & s \in \partial U \end{cases}$$

where E_s denotes the expectation of functionals, given the initial condition s, and I denotes the indicator function. The function $V(s)$ can be interpreted as the probability that a trajectory starting at s will reach set T while avoiding set U.

If the state hits the boundary of the unsafe or target set, then the value function will take the value 0 and 1, respectively, and it is assumed that the execution of the SHS terminates. The termination of the stochastic process is formalized by slightly modifying the SHS model. Inspired by [14], we add a new terminal state Δ. The system transitions to Δ with a probability of 1 only upon hitting the boundary of the target or unsafe set. The transition to the terminal state is captured by extending the transition measure R of the SHS according to the following:

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

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 immediately dies after transitioning to Δ, i.e., $b(\Delta) = \sigma(\Delta) = \lambda(\Delta) = 0$. Finally, we extend V 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 $s(t)$.

Given the assumptions on sets T and U and their boundaries, we can construct a bounded function $c : \bar{S} \to \mathbb{R}_+$ continuous

in x such that

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

We define a counting process p^* by

$$p^*(t)=\sum_{i=1}^{\infty} I_{(t\geq t_i)}I_{\left(s(t_{i^-})\in\partial S\right)}.$$

Process $p^*(t)$ counts the number of times the trajectory hits the boundary and jumps up to time t [14]. Then, value function V can be written as

$$V(s)=E_s\left[\int_0^{\infty} c\left(q_{t^-},x_{t^-}\right)dp^*(t)\right]. \tag{2}$$

We will show that V can be characterized as a viscosity solution of a system of coupled HJB equations.

The formulation of the reachability problem previously described can be modified to describe safety. In a safety problem, we are given a set of safe states, and we want to compute the probability that the system execution from an arbitrary (safe) initial state will go outside the safe set. Let $B=\cup_{q\in Q_B}\{q\}\times B^q$ be a subset of S representing the set of safe states. The safety problem is shown in Fig. 1(b). We assume that the set of unsafe states $X^q\setminus B^q$ for each q is a proper subset of X^q, i.e., $\partial X^q\cap\partial B^q=\emptyset$. The initial state must lie inside the safe set B, 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. We can transform the safety problem to a reachability problem by defining the target set as $T^q=X^q\setminus B^q$ and the unsafe set as $U^q=\emptyset$. Note that, in this case, the definition of Γ^q becomes $\Gamma^q=X^q\setminus(T^q\cap U^q)=B^q$. Clearly, with this transformation, the probability that the system is unsafe can be computed as the value function described by (2) similarly to the reachability problem.

B. Viscosity Solutions

In this section, we use a dynamic programming argument to derive a representation of the value function that resembles a discount cost criterion with a target set. Then, we extend the results from standard stochastic diffusions to show that the value function is characterized as a viscosity solution of a system of HJB equations.

The application of dynamic programming requires a recursive scheme that provides the basis for computing the value function. We consider the set of nonnegative Borel measurable functions $\mathcal{B}(S)_+$ and define operator $\mathcal{G}:\mathcal{B}(S)_+\to\mathcal{B}(S)_+$ by

$$\mathcal{G}g(q,x)=E_s\left[c\left(q_{t_1^-},x_{t_1^-}\right)I_{\left(t_1=t_1^*\right)}+g\left(q_{t_1},x_{t_1}\right)\right] \tag{3}$$

where t_1 is the stopping time of the first jump. The value function can be computed by recursive application of operator $\mathcal{G}$. The recursion is defined with respect to the stopping times t_i that represent the times of the discrete jumps. The next lemma defines the recursive operation of $\mathcal{G}$ and is used by Theorem 1, which shows that value function V is a fixed point of $\mathcal{G}$.

Lemma 1:

$$\mathcal{G}^n g(q,x)=E_s\left[\int_0^{t_n} c\left(q_{t^-},x_{t^-}\right)dp^*(t)+g\left(q_{t_n},x_{t_n}\right)\right].$$

Proof: By the strong Markov property [7] and the construction of the SHS process, we have[4]

$$\begin{aligned}&E_s\left[c\left(q_{t_2^-},x_{t_2^-}\right)I_{\left(t_2=t_2^*\right)}+g\left(q_{t_2},x_{t_2}\right)|\mathcal{F}_{t_1}\right]\\&\quad=E_s\left[c\left(q_{t_1},x_{t_2^-}\right)I_{\left(t_2=t_2^*\right)}+g\left(q_{t_2},x_{t_2}\right)|\mathcal{F}_{t_1}\right]\\&\quad=E_s\left[g\left(q_{t_1},x_{t_1}\right)\right].\end{aligned}$$

Therefore

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

By induction, we get

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

■

Theorem 1: Value function V is a fixed point of operator $\mathcal{G}$.

Proof: By definition of $\mathcal{G}$, for any $\psi_1\leq\psi_2$, we have $\mathcal{G}\psi_1\leq\mathcal{G}\psi_2$. 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, $\{v^n\}$ monotonically increases, and v^n takes values in [0, 1] 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 $v\geq v^n$, we have $\mathcal{G}v\geq\mathcal{G}v^n$. Thus, $\mathcal{G}v\geq v^{n+1}$ for all n. Therefore, $\mathcal{G}v\geq v$. In addition, $\mathcal{G}v^n=v^{n+1}\leq v\leq\mathcal{G}v$, and $\lim_{n\to\infty}v^n=v$. Therefore, $\mathcal{G}v\leq v\leq Gv$, and $v=\lim_{n\to\infty}v^n$ is a fixed point of $\mathcal{G}$.

Finally, by Lemma 1, $v=\lim_{n\to\infty}G^nv^0=E_s[\int_0^{\infty}c(q_{t^-},x_{t^-})dp^*(t)]$; therefore, V is a fixed point of $\mathcal{G}$, i.e., $V(s)=\mathcal{G}V(s)$. ■

Next, we show that value function V for the reachability problem of SHSs is similar to the value function for the exit problem of a standard stochastic diffusion, but the running and terminal costs depend on value function V itself.

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

Theorem 2: Consider the value function $V(s)$ defined by (2), and define $L^V(q,x) = \lambda(q,x)\int_\Gamma V(y)R((q,x),dy)$ and $\psi^V(q,x) = c(q,x) + \int_\Gamma V(y)R((q,x),dy)$. Denote $\Lambda(t) = \exp\{-\int_0^t \lambda(q_0,x_z)dz\}$; then, for $s \in \Gamma$

$$V(s) = E_s\left[\int_0^{t_1^*} \Lambda(t)L^V\left(q_{t^-},x_{t^-}\right)dt + \Lambda\left(t_1^*\right)\psi^V\left(q_{t_1^*},x_{t_1^*}\right)\right]. \tag{4}$$

Proof: The SHS satisfies the strong Markov property [7]; 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 and $t_1^* = \inf\{t \geq 0 : x(t) \in \partial X^{q(t_0)}\}$; then, using a standard dynamic programming argument, we can write

$$V(s) = E_s\left[I_{\left(t_1<t_1^*\right)}\int_\Gamma V(y)R\left(\left(q_{t_1^-},x_{t_1^-}\right),dy\right) + I_{\left(t_1=t_1^*\right)}\left(c\left(q_{t_1^*},x_{t_1^*}\right) + \int_\Gamma V(y)R\left(\left(q_{t_1^*},x_{t_1^*}\right),dy\right)\right)\right]. \tag{5}$$

By construction of the transition rate λ, t_1, and x_t are not independent (unless λ is constant). Denote the σ-field $\sigma(x_t, t \geq 0)$ generated by x_t as $\mathcal{F}_\infty$. The conditional distribution of t_1, given $\mathcal{F}_\infty$, is

$$P[t_1 > t|\mathcal{F}_\infty] = I_{t<t_1^*}\Lambda(t)$$

and the conditional density of t_1 is

$$\frac{dP[t_1 \leq t|\mathcal{F}_\infty]}{dt} = \lambda(q_0,x_t)\Lambda(t)I_{\left(t<t_1^*\right)} + \Lambda\left(t_1^*\right)\delta\left(t-t_1^*\right).$$

Thus, (5) can be written as

$$\begin{aligned} V(s) &= E_s\left[E_s\left[I_{\left(t_1<t_1^*\right)}\int_\Gamma V(y)R\left(\left(q_{t_1^-},x_{t_1^-}\right),dy\right) + I_{\left(t_1=t_1^*\right)}\left(c\left(q_{t_1^*},x_{t_1^*}\right) + \int_\Gamma V(y) \times R\left(\left(q_{t_1^*},x_{t_1^*}\right),dy\right)\right)|\mathcal{F}_\infty\right]\right] \\ &= E_s\left[\int_0^{t_1^*}\lambda(q_t,x_t)\Lambda(t)\int_\Gamma V(y)R\left((q_{t^-},x_{t^-}),dy\right)dt + \Lambda\left(t_1^*\right)c\left(q_{t_1^*},x_{t_1^*}\right) + \Lambda\left(t_1^*\right) \times \int_\Gamma V(y)R\left(\left(q_{t_1^*},x_{t_1^*}\right),dy\right)\right] \end{aligned}$$

and, using the definitions of $L^V(q,x)$ and $\psi^V(q,x)$, we have

$$V(s) = E_s\left[\int_0^{t_1^*}\Lambda(t)L^V\left(q_{t^-},x_{t^-}\right)dt + \Lambda\left(t_1^*\right)\psi^V\left(q_{t_1^*},x_{t_1^*}\right)\right].$$

■

Assuming that 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 [34]. Then, if V is continuous in $\bar{X}^{q(t_0)}$, (4) is similar to the discounted cost criterion with a target set of a standard stochastic diffusion [3]. The main difference is that running cost $L^V(q,x)$ and terminal cost $\psi^V(q,x)$ depend on the value function. It should be noted that, since the SHS satisfies the strong Markov property, the same procedure can be repeated every time a jump occurs. Next, we show that, under the nondegeneracy assumption, V is bounded and continuous.

Theorem 3: V is bounded and continuous in x on $\bar{\Gamma}$.

Proof: The $\mathcal{G}$ operator defined by (3) can be written as

$$\mathcal{G}g(q,x) = E_s\left[\int_0^{t_1} c(q_{t^-},x_{t^-})dp^*(t) + g\left(q_{t_1},x_{t_1}\right)\right].$$

Since the SHS satisfies the strong Markov property, we can apply the same transformation as in Theorem 2 to get

$$\mathcal{G}g(q,x) = E_s\left[\int_0^{t_1^*}\Lambda(t)L^g(q_{t^-},x_{t^-})dt + \Lambda\left(t_1^*\right)\psi^g\left(q_{t_1^*},x_{t_1^*}\right)\right] \tag{6}$$

and therefore

$$\begin{aligned} v^{n+1}(q,x) &= \mathcal{G}v^n(q,x) \\ &= E_s\left[\int_0^{t_n^*}\Lambda(t)L^{v^n}(q_{t^-},x_{t^-})dt + \Lambda(t_1^*)\psi^{v^n}(q_{t_n^*},x_{t_n^*})\right]. \end{aligned}$$

Because of the nondegeneracy assumption, the exit times t_i^* are continuous at the sample paths of the process [3]. Therefore, all the functions in the sequence v^n are continuous, and furthermore, we have $v^n \geq v^0$ for every n. By applying the results in [34, Ch. 7], we can conclude that $V = \lim_{n\to\infty} v^n$ is lower semicontinuous and bounded below.

Next, define a new function $\tilde{V} : \bar{\Gamma} \to \mathbb{R}_+$ by

$$\tilde{V}(s) = \begin{cases} E_s\left[I_{(s(\tau^-)\in\partial U)}\right], & s \in \Gamma \\ 1, & s \in \partial U \\ 0, & s \in \partial T. \end{cases}$$

Function $\tilde{V}$ can be interpreted as the probability that a trajectory starting at s will reach U before T, and it can be written as

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

where

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

From the nondegeneracy assumption, we have $\tilde{V} = 1 - V(s)$. By applying the argument given in the beginning of the proof to $\tilde{V}$, it follows that $\tilde{V}$ is lower semicontinuous and bounded below; therefore, $V = 1 + (-\tilde{V})$ is upper semicontinuous and bounded above. Thus, V is continuous and bounded in $\bar{\Gamma}$. ■

Next, we prove the main result of this section that characterizes V as the viscosity solution of a system of HJB equations. The HJB equations are derived based on the results of [3] and [4].

Theorem 4: Assume that b and σ are continuously differentiable with respect to x in Γ^q for each q and, for suitable C_1 and C_2, satisfy $|b_x| \leq C_1$, $|\sigma_x| \leq C_1$, and $|b(q,0)| + |\sigma(q,x)| \leq C_2$. Then, V is the unique viscosity solution of the following system of equations:

$$\mathcal{H}_V\left((q,x), V, D_xV, D_x^2V\right) = 0 \text{ in } \Gamma^q, \qquad q \in Q \tag{7}$$

with boundary conditions

$$V(q,x) = \psi^V(q,x) \text{ on } \partial\Gamma^q, \qquad q \in Q \tag{8}$$

where

$$\mathcal{H}_V\left((q,x), V, D_xV, D_x^2V\right) = b(q,x)D_xV + \frac{1}{2}\operatorname{tr}\left(a(q,x)D_x^2V\right) + \lambda(q,x)V + L^V(q,x).$$

Proof: Consider the function

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

where $g \in \mathcal{B}(S)_+$ is a continuous and bounded function. From (6), it follows that $v(q,x)$ is the value function of an exit-time problem in Γ^q for the diffusion (1), where $L^g : \Gamma \to \mathbb{R}_+$ and $\psi^g : \partial\Gamma \to \mathbb{R}_+$ are bounded continuous functions. Under the assumptions of f and σ, we can apply the results for standard Markov diffusions [4, Th. V.2.1, Corollary V.3.1]; therefore, $v(q,x)$ is a viscosity solution of

$$\mathcal{H}_g\left((q,x), V, D_xV, D_x^2V\right) = 0 \text{ in } \Gamma^q \tag{9}$$

$$V(q,x) = \psi^g(q,x) \text{ on } \partial\Gamma^q. \tag{10}$$

By Theorem 3, V is bounded and continuous. Therefore

$$\bar{V}(q,x) = \begin{cases} \mathcal{G}V(q,x), & \text{in } \Gamma^q \\ \psi^V(q,x), & \text{on } \partial\Gamma^q \end{cases}$$

is a viscosity solution of

$$\mathcal{H}_V\left((q,x), \bar{V}, D_x\bar{V}, D_x^2\bar{V}\right) = 0 \text{ in } \Gamma^q$$

$$\bar{V}(q,x) = \psi^V(q,x) \text{ on } \partial\Gamma^q$$

where V is considered to be known, and $\bar{V}$ is unknown. However, V is a fixed point of $\mathcal{G}$; thus, $V = \mathcal{G}V = \bar{V}$ in Γ^q, and $\psi^V = \psi^{\bar{V}}$ on $\partial\Gamma^q$, which means that $V = \bar{V}$ is a viscosity solution of (7) and (8). Furthermore, V is continuous and therefore is the unique viscosity solution, which is continuous on $\bar{\Gamma}$. ■

Equation (7) describes a set of coupled second-order partial differential equations (one for each discrete state), with boundary conditions given by (8), which can be viewed as a set of HJB equations associated with the reachability problem for the SHS. The coupling between the equations arises because the value function in a particular mode depends on the value function in the adjacent modes and is formally captured by the dependence of the running and terminal costs $L^V(q,x)$ and $\psi^V(q,x)$ on value function V.

V. Numerical Methods for Reachability Analysis

A. Locally Consistent MCs

In this section, we employ the finite-difference method presented in [3] to compute locally consistent MCs that approximate the SHS while preserving local mean and variance. We consider a discretization of the state space denoted by $\bar{S}^h = \cup_{q\in Q}\{q\} \times \bar{S}_q^h$, where $\bar{S}_q^h$ is a set of discrete points approximating X^q and $h > 0$ is an approximation parameter characterizing the distance between neighboring points. By abuse of notation, we denote the sets of boundary and interior points of $\bar{S}_q^h$ as ∂S_q^h and S_q^h, respectively. By the boundness assumption, the approximating MC will have finitely many states, which are denoted by $s_n^h = (q_n^h, \xi_n^h)$, $n = 1, 2, \ldots, N$.

First, we consider the continuous evolution of the SHS between jumps and assume that the state is (q,x). The local mean and variance given by the SDE (1) on interval $[0,\delta]$ are

$$E\left[x(\delta) - x\right] = b(q,x)\delta + o(\delta)$$

$$E\left[\left(x(\delta) - x\right)\left(x(\delta) - x\right)^T\right] = a(q,x)\delta + o(\delta).$$

Let $\{q_n^h = q, \xi_n^h\}$ describe the MC on $S_q^h \subset X^q$ with transition probabilities denoted by $p_D^h((q,x),(q',x'))$. A locally consistent MC must satisfy

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

$$E\left[\left(\Delta\xi_n^h - E\left[\Delta\xi_n^h\right]\right)\left(\Delta\xi_n^h - E\left[\Delta\xi_n^h\right]\right)^T\right] = a(q,x)\Delta t^h(q,x) + o\left(\Delta t^h(q,x)\right)$$

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 diffusion transition probabilities $p_D^h((q,x),(q',x'))$ and the interpolation intervals can be systematically computed from the parameters of the SDE (details can be found in [3]). For example, if the diffusion matrix $a(q,x)$ is diagonal and we consider a uniform grid, with e_i denoting the unit vector in the ith direction, the transition probabilities are

$$p_D^h\left((q,x),(q,x \pm he_i)\right) = \frac{a_{ii}(q,x)/2 + hb_i^{\pm}(q,x)}{Q(q,x)}$$

and the interpolation intervals are $\Delta t(q,x) = h^2/Q(q,x)$, where $Q(q,x) = \sum_i [a_{ii}(q,x) + h|b_i(q,x)|]$, and $a^+ = \max\{a,0\}$ and $a^- = \max\{-a,0\}$ denote the positive and negative parts of a real number, respectively.

Next, we consider the jumps with transition rate $\lambda(q,x)$ and transition measure $R((q,x),A)$. Suppose that, at time t, the state has just changed to $\{q_n^h = q, \xi_n^h = x\}$. The probability that

a jump will occur on $[t, t+\delta)$ conditioned on the past data can be approximated by

$$P\left[(q,x) \text{ jumps on } [t,t+\delta) | q(s), x(s), w(s), s \le t\right] = \lambda(q,x)\delta + o(\delta).$$

The ith jump of the approximating process is denoted by $\zeta((q,x),\rho_i)$, where ρ_i are independent random variables with distribution $\bar{R} = \{\rho : \zeta((q,x),\rho_i) \in A\} = R((q,x),A)$ with compact support Π. Let ζ^h be a bounded measurable function such that $|\zeta^h((q,x),\rho) - \zeta((q,x),\rho)| \to 0$ as $h \to 0$ uniformly in x for each ρ, which satisfies $\zeta^h((q,x),\rho) \in \bar{S}^h$.

If $x \in S_q^h$, then, with probability $p^h_{\text{jump}}(q,x) = \lambda(q,x)\Delta t^h(q,x) + o(\Delta t^h(q,x))$, there is a jump, and the next state is $(q^h_{n+1}, \xi^h_{n+1}) = \zeta^h((q,x),\rho_i)$; with probability $1 - p^h_{\text{jump}}(q,x)$, the next state is determined by the diffusion probabilities p^h_D. Thus, the transition probabilities are given by

$$p^h\left((q,x),(q',x')\right) = \left(1 - p^h_{\text{jump}}(q,x)\right) p^h_D\left((q,x),(q',x')\right) + p^h_{\text{jump}}(q,x)\bar{R}\left\{\rho : \zeta^h\left((q,x),\rho\right) = (q', x' - x)\right\}. \quad (11)$$

For points $x \in \partial S_q^h$ in the boundary, the next state is determined by $\zeta^h((q,x),\rho_i)$ with a probability of 1, and the transition probabilities are given by

$$p^h\left((q,x),(q',x')\right) = \bar{R}\left\{\rho : \zeta^h\left((q,x),\rho\right) = (q', x' - x)\right\}. \quad (12)$$

B. Iterative Methods for Reachability Analysis

The previous section described how we can approximate an SHS by a locally consistent MC. This section describes the approximation of the value function, formulates the discrete verification problem, and presents the convergence results for the numerical methods based on the discrete approximations.

We consider the approximating MC $\{s^h_n\} = \{(q^h_n, \xi^h_n)\}$ with transition probabilities $p^h((q,x),(q',x'))$ defined in (11) and (12). Let $\bar{T}^h = \bar{S}^h \cap \bar{T}$ and $\bar{U}^h = \bar{S}^h \cap \bar{U}$ denote the discretized target and unsafe sets, respectively. We denote the times of the jumps between modes as n_i and the stopping time representing $(q^h_n, \xi^h_n) \in \bar{T}^h \cup \bar{U}^h$ as ν_h. Then, value function V can be approximated by

$$V^h(s) = E_s\left[\sum_{n=0}^{\nu_h} c\left(q^h_n, \xi^h_n\right) I_{(n=n_i)}\right].$$

Function V^h can be computed using a value iteration algorithm. To show the convergence of the algorithm, we modify the model to capture the termination of the process by considering a terminal state Δ similar to Section IV. The state space of the MC becomes $\tilde{S}^h = \bar{S}^h \cup \{\Delta\}$, and the transition probabilities are defined, so that $\tilde{p}^h((q,x),\Delta) = 1$ if $x \in \bar{T}^h \cup \bar{U}^h$, $\tilde{p}^h(\Delta,\Delta) = 1$, and $\tilde{p}^h((q,x),(q',x')) = p^h((q,x),(q',x'))$ otherwise. This means that, when the state reaches T or U, it transitions to Δ and stays there forever. Consider the function $\tilde{c} : \tilde{S}^h \to \mathbb{R}_+$ with $\tilde{c}(\Delta) = 1$ and $\tilde{c}(q,x) = 0$ for every (q,x), and the value function

$$\tilde{V}^h(s) = E_s\left[\sum_{n=0}^{\infty} \tilde{c}\left(s^h_n\right)\right]. \quad (13)$$

Clearly, this sum is well-defined and bounded, and we have $\tilde{V}^h = V^h$. The next proposition shows that function $\tilde{V}^h$ can be computed using value iteration assuming appropriate initial conditions.

1) Proposition 1: Let $\tilde{V}^h_0(q,x) = 0$ for every (q,x); then, the iteration

$$\tilde{V}^h_{n+1}(q,x) = \left[\sum_{q',x'} \tilde{p}^h\left((q,x),(q',x')\right) \tilde{V}^h_n(q',x')\right] \quad (14)$$

converges pointwise and monotonically to $\tilde{V}^h = V^h$.

Proof: Consider the value function defined by (13). We have $\tilde{V}^h(q,x) \in [0,1]_< \infty$ and $\tilde{c}(s) \ge 0$ for all $s \in \tilde{S}^h$. Therefore, computing $\tilde{V}$ is a special case of the total expected reward criterion for positive models [21]. If v is a fixed point of the iteration (14), then $v + k[1,\ldots,1]^T$, $k > 0$, is also a fixed point. Thus, the iteration may have multiple fixed points, but if we pick $\tilde{V}^h_0 = 0$, it converges to the least fixed point $\tilde{V}^h$ [21, Th. 7.2.12]. ■

C. Convergence Results

Finally, we show that the value function V^h obtained using the approximating MC converges to the value function V of the SHS as $h \to 0$. The proof of the convergence is a straightforward extension to the SHSs of the results presented in [4].

Let $g \in \mathcal{B}(S)_+$ be a continuous and bounded function, and suppose that V is the unique viscosity solution of (9) and (10) that is bounded and continuous in $\bar{\Gamma}^q$. First, we show convergence for V^h when the boundary conditions are described by function g.

We consider $\bar{\Sigma}^h_q$ to be a discretization of $\bar{\Gamma}^q$ and denote the set of interior and boundary points as Σ^h_q and $\partial\Sigma^h_q$, respectively. The dynamic programming equation can be written as

$$V^h(q,x) = \begin{cases} F^h_g\left[V^h(\cdot)\right](q,x), & \text{if } x \in \Sigma^h_q \\ \psi^h_g(q,x), & \text{if } x \in \partial\Sigma^h_q \end{cases}$$

where

$$F^h_g[V^h(\cdot)](q,x) = \left(1 - p^h_{\text{jump}}(q,x)\right) \times \sum_{q',x'} p^h_D\left((q,x),(q',x')\right) V^h(q',x') + \left(p^h_{\text{jump}}(q,x)\right) \int_{\Pi} g(\zeta_h\left((q,x),\rho\right)) \bar{R}(d\rho)$$

$$\psi^h_g(q,x) = c(q,x) + \int_{\Pi} g\left(\zeta^h((q,x),\rho)\right) \bar{R}(d\rho).$$

Lemma 2: $\lim_{y\to x, h\to 0} V^h(q,y) = V(q,x)$ uniformly in $\bar{\Gamma}^q$.

Proof: V is the continuous and bounded viscosity solution of (9) and (10), and $\psi^g(q,x)$ is continuous. Therefore, for each q, we have a standard exit problem from Γ^q for the SDE (1), and by applying the results of [4, Sec. IX5], V^h converges uniformly to V. ■

To show the convergence of V^h for the SHS, we replace g by V, and we follow an argument similar to the proof of Theorem 4.

Theorem 5: Let

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

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

Proof: Assume that V is given, and define

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

By Lemma 2, 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; therefore, $\bar{V}^h=V^h$ for every h and $\bar{V}=V$. ■

D. Complexity Analysis

So far, we have proven that the iteration described by (14) converges to the value function V^h for zero initial conditions and, furthermore, that V^h converges to value function V, i.e., the viscosity solution for the original SHS problem, as the discretization becomes finer. Next, we show that the proposed computational algorithm is polynomial in the number of states of the approximating discrete Markov process.

Analysis of the computational complexity of value iteration algorithms is usually based on the contraction property of the iteration operator. The iteration operator used for verification of SHS corresponds to an undiscounted criterion, and showing that it is a contraction mapping is more complex. In this section, we prove first that the iteration operator restricted to an appropriate set is a contraction mapping with respect to some weighted infinity norm. Based on the contraction property, we conclude the polynomial-time complexity of the algorithm. Our analysis is based on the methodology presented in [32] and [35].

We consider the MC $\{s_n^h=(q_n^h,\xi_n^h), n=1,2,\ldots,N\}$ with state space denoted by $\tilde{S}^h$ derived earlier in this section and denote the iteration operator defined by (14) as $\tilde{F}^h$. By construction of terminal state Δ, if the chain reaches ∂T^h or ∂U^h, it transitions to Δ with a probability of 1. States from which Δ cannot be reached do not affect the convergence of the value iteration algorithm. The value function for these states is initialized to 0 and will remain 0 as the algorithm proceeds. Without loss of generality, we index the states as follows: the first state s_1^h is the terminal state Δ, states $s_n^h, n=2,\ldots,M$ are the states from which Δ can be reached, and s_n^h, $n=M+1,\ldots,N$ are the states from which Δ cannot be reached.

Lemma 3: The operator $\tilde{F}^h:\mathbb{R}^N\to\mathbb{R}^N$ defined by (14) is a contraction mapping with respect to some weighted norm $\|\cdot\|_\infty^w$ over $X=\{x\in\mathbb{R}^N | x\geq 0,\ x_1=x_{M+1}=\cdots=x_N=0\}$.

Proof: We consider the set $\Theta=\{s_n^h, n=1,2,\ldots,M\}$, and we construct the following partition:

$$\begin{aligned}\Theta_1&=\left\{s_1^h\right\}\\ \Theta_k&=\left\{s_n^h | s_n^h\notin\Theta_1\cup\cdots\cup\Theta_{k-1} \text{ and } \right.\\ &\qquad\left.\exists s_m^h\in\Theta_1\cup\cdots\cup\Theta_{k-1} \text{ s.t. } \tilde{p}^h\left(s_n^h,s_m^h\right)>0\right\}.\end{aligned}$$

Clearly, for every state $s_n^h\in\Theta$, there exists some k such that $s_n^h\in\Theta_k$. In addition, for every k and every state $s_n^h\in\Theta_k$, we have $s_n^h\in\Theta$; therefore, there exists L such that $\bigcup_{k=1}^L\Theta_k=\Theta$.

We define weights $w_2,\ldots,w_M$ as follows:

$$w_n=\begin{cases}1-\eta^{2k}, & \forall s_n^h\in\Theta_k, k=1,\ldots,L\\ 1, & \text{otherwise}\end{cases}$$

where $\eta=\min_{s_m^h:\tilde{p}^h(s_n^h,s_m^h)>0}\{\tilde{p}^h(s_n^h,s_m^h)>0\}$. Since $\eta\in(0,1)$, we have $w_n\in(0,1)$ for every $n=1,\ldots,M$. Let $\gamma=(1-\eta^{2L-1})/(1-\eta^{2L+1})<1$. Consider state $s_n^h\in\Theta_k$, and let $s_\ell^h\in\Theta_1\cup\cdots\cup\Theta_{k-1}$ such that $\tilde{p}^h(s_n^h,s_\ell^h)>0$. We have

$$\begin{aligned}&\left(\sum_{s_m^h\in\Theta}\tilde{p}^h\left(s_n^h,s_m^h\right)w_m\right)\Big/w_n\\ &\leq\left(\sum_{s_m^h\in\Theta\setminus\left\{s_\ell^h\right\}}\tilde{p}^h\left(s_n^h,s_m^h\right)+\tilde{p}^h\left(s_n^h,s_m^h\right)w_\ell\right)\Big/w_n\\ &=\left(1+\tilde{p}^h\left(s_n^h,s_m^h\right)(w_\ell-1)\right)/w_n\\ &\leq\left(1+\eta(w_\ell-1)\right)/w_n\\ &\leq(1-\eta^{2k-1})/w_n\\ &=(1-\eta^{2k-1})/(1-\eta^{2k})\\ &\leq\gamma\end{aligned}$$

where the first inequality follows from the fact that $w_m\in(0,1)$, the second inequality follows from $\tilde{p}^h(s_n^h,s_m^h)\geq\eta$, and the third inequality follows from $w_\ell\leq 1-\eta^{2k-2}$ since $s_\ell^h\in\Theta_1\cup\cdots\cup\Theta^{k-1}$.

This implies that, for any state s_n^h and $x,y\in X$

$$\begin{aligned}&\tilde{F}^h[x]\left(s_n^h\right)-\tilde{F}^h[y]\left(s_n^h\right)\\ &\leq\sum_{s_m^h}\tilde{p}^h\left(s_n^h,s_m^h\right)\left(x\left(s_m^h\right)-y\left(s_m^h\right)\right)\\ &=\sum_{s_m^h\neq s_\ell^h,\ell=1,M+1,\ldots,N}\tilde{p}^h\left(s_n^h,s_m^h\right)w_m\left(x\left(s_m^h\right)-y\left(s_m^h\right)\right)/w_m\\ &\leq\gamma w_n\max_{s_m^h}\left\{\left(x\left(s_m^h\right)-y\left(s_m^h\right)\right)/w_m\right\}.\end{aligned}$$

Similarly

$$\tilde{F}^h[y]\left(s_n^h\right)-\tilde{F}^h[x]\left(s_n^h\right)\leq\gamma w_n\max_{s_m^h}\left\{\left(x\left(s_m^h\right)-y\left(s_m^h\right)\right)/w_m\right\}.$$

Therefore

$$\left\|\tilde{F}^h[x]\left(s_n^h\right)-\tilde{F}^h[y]\left(s_n^h\right)\right\|_\infty^w\leq\gamma\|x-y\|_\infty^w$$

where $\|x\|_\infty^w=\|(x_1,x_2/w_2,\ldots,x_M/w_M,x_{M+1},\ldots,x_N\|_\infty$, i.e., the operator $\tilde{F}^h$ is a contraction mapping with modulus γ. ■

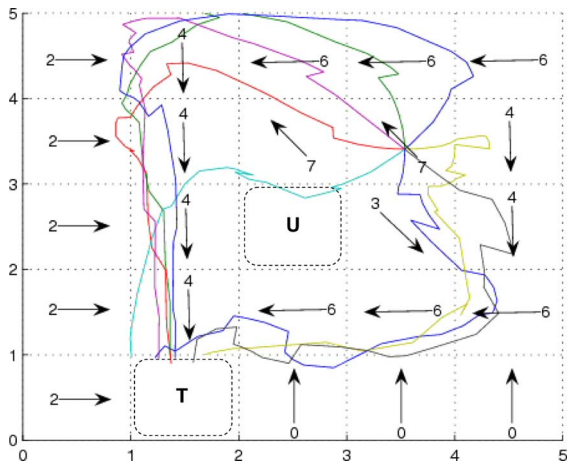

Fig. 2. Navigation benchmark.

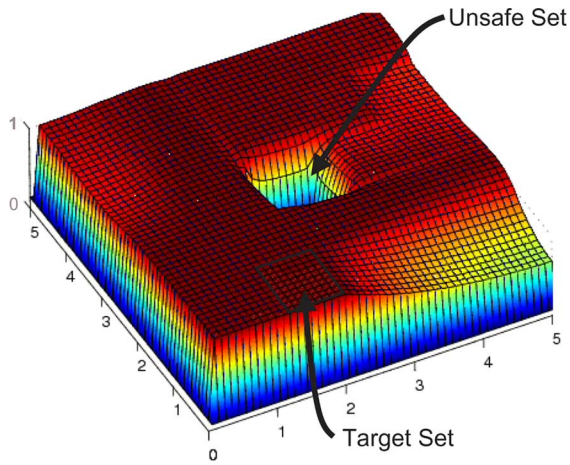

Fig. 3. Value function for the navigation benchmark.

Theorem 6: The iteration defined by (14) converges to the desired value function in a number of steps that are polynomial in the number of states N of the discrete approximation process $\{s_n^h, n = 1, \ldots, N\}$ and the number of bits used to represent the parameters of the process.

Proof: By the previous lemma, $\tilde{F}^h$ is a contraction mapping, and the successive estimates $\tilde{V}_n^h$ geometrically converge to a fixed point $\tilde{V}^h$. By Theorem 5, $\tilde{V}^h$ is the desired solution since it converges as $h \to 0$ to the viscosity solution V that characterizes the safety of the SHS. Since $\tilde{F}^h$ is a contraction mapping, by applying the results in [35, Lemma 1], the value function converges in a number of steps that are polynomial in the number of states N of the discrete approximation process and the number of bits used to represent the parameters of the process. ■

Reachability analysis of SHSs is polynomial in the number of states of the approximating Markov process; however, this number exponentially grows with the dimension of the continuous state space. Therefore, application of the approach is limited to low-dimensional systems. Although scalability is a limiting factor, using parallel methods, the approach is feasible for realistic systems. For example, the approach has been applied for safety analysis of sugar cataract development to a 7-D biochemical system for which the approximating process has approximately 700 million states [31].

VI. Benchmarks

This section presents experimental results for two benchmarks that have been proposed for verification of hybrid systems.

A. Navigation Benchmark

We first illustrate our approach using a stochastic version of the navigation benchmark presented in [5]. The benchmark describes an object moving within a bounded 2-D region partitioned into cells X^q, $q \in \{0, 1, \ldots, N_c\}$, as shown in Fig. 2. Let $x = [x_1, x_2]^T$ and $v = [v_1, v_2]^T$ denote the position and velocity of the object, respectively. The behavior is defined by the ordinary differential equation $\dot{v} = A(v - v_d^q)$, where $A \in \mathbb{R}^{2\times 2}$ and $v_d^q = [\sin(q\pi/4), \cos(q\pi/4)]^T$. Selecting matrix A and adding a diffusion term, the dynamics of the object are described by the SDE

$$dx = \left(\tilde{A}x + \tilde{B}u_d^q\right) dt + \Sigma dw$$

where $x = [x_1, x_2, v_1, v_2]^T$, $u_d^q = [0, 0, v_d^q]^T$, and $w(t)$ is an $\mathbb{R}^4$-valued Wiener process

$$\tilde{A} = \begin{bmatrix} 0 & I_2 \\ 0 & A \end{bmatrix} \quad A = \begin{bmatrix} -1.2 & 0.1 \\ 0.1 & -1.2 \end{bmatrix} \quad \Sigma = 0.1 I_4$$

Consider the target set T and the unsafe set U shown in Fig. 2. Given an initial state $s_0 = (q_0, x_0)$, we want to compute the probability that the state will reach T while avoiding U. Fig. 2 also shows sample trajectories. In order to apply the approach described in this paper, we underapproximate each cell X^q by $\tilde{X}^q$ by considering a smooth boundary $\partial\tilde{X}^q$. We also define a transition measure $R((q, x), A)$, so that the state jumps into an adjacent cell if it hits an "inner" boundary and jumps into the same cell if it hits an "outer" boundary. The transition rate is assumed to be zero. We discretize the state space using a uniform grid with approximation parameter $h > 0$ and apply the method described in Section V to compute $V^h(q, x)$. As $h \to 0$, $V^h(q, x)$ converges to the solution $V(q, x)$ of the stochastic approximation of the benchmark problem.

Since the continuous state space of the example is 4-D, we select to plot a projection of V^h for initial velocity $v_0 = [0, 0]^T$. Fig. 3 shows this projection for $h = 0.1$ that describes the probability that a trajectory starting from $(q, [x_1, x_2, 0, 0]^T)$ will reach T while avoiding U. The computational performance of the algorithm is illustrated in Table I. All data were collected using a 3.0-GHz desktop computer with 1-GB random access memory, and they are consistent with the polynomial-time complexity of the algorithm.

B. Room Heater Benchmark

A modeling benchmark of a room-heating problem has been presented for a simple three-room system in [5]. The benchmark models the temperature dynamics of a building with three rooms and two mobile heaters. The temperature in each

TABLE I
PERFORMANCE DATA

h	Time (minutes)	Number of States
.5	.5	2500
.25	7	32400
.1	200	1147041
.05	5110	17147881

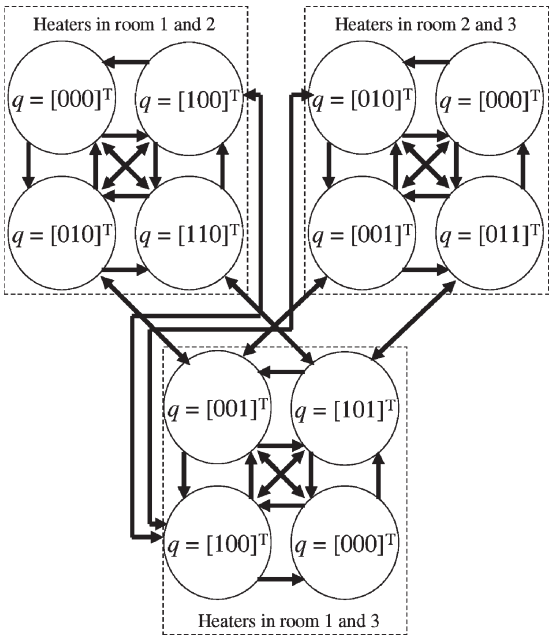

Fig. 4. Automaton for the room heater benchmark.

room x_i depends on the temperature of the adjacent rooms, the outside temperature u, and whether a heater is in the room and turned on.

We have generated a stochastic version of the benchmark. The SDE describing the continuous dynamics of the system is

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

where

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

$C = \mathrm{diag}(6, 7, 8)$, $u = 4$, $\Sigma = \mathrm{diag}(0.1)$, q is a vector consisting of 0s and 1s representing the position and state of the heaters, 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 turned on, then a 1 is placed in the corresponding position of that room. If the heater is not in the room or is in the room but turned off, then a 0 is placed in the corresponding position. The heating benchmark has 12 heater modes, as shown in Fig. 4. Mode transitions are denoted by the arcs between nodes and are defined using a control policy for moving the heater. The control policy is captured by the invariants of the discrete states. We consider the following control policy for rooms i and j. If a heater is present in room i but is turned off, it is switched on if $x_i \leq 19$ and a heater that is on is switched off if $x_i \geq 20$. A heater is moved from room j to an adjacent room i if the following conditions are true: 1) room i is without a heater; 2) room j currently has a heater; 3) $x_i \leq 17$; and 4) $x_j - x_i \geq 1$.

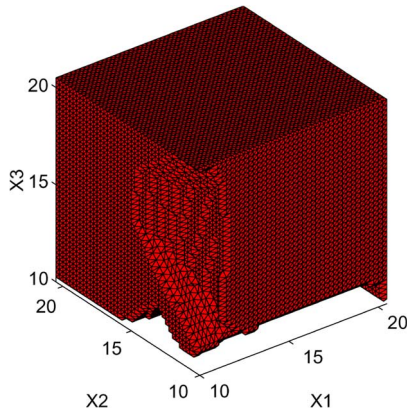

Fig. 5. Room heater benchmark safe states for $q = [110]^T$.

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 $h = 0.25$. Since there are 12 discrete modes, the number of states of the approximating process is $12 \times 42^3 = 889\,056$ (including the boundary of the safe set). The room heater benchmark evolves in a 3-D continuous state space; hence, it is difficult to visualize the value function. To illustrate our results, we have set a predefined threshold (0.1) that describes the acceptable probability of 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. Fig. 5 shows the safe set. The iterative algorithm executed in approximately 49 min on a 3.0-GHz desktop computer.

An important characteristic of the room heater benchmark is that it can be easily scaled up to an arbitrary number of rooms that determine the dimension of the continuous state space. Using parallel methods for dynamic programming [32], we have verified a 6-D version of the room heater benchmark. For approximation parameter $h = 0.25$, the discrete approximation was verified in approximately 10^3 min in a high-performance computer cluster with four processors.

VII. CONCLUSION AND FUTURE WORK

This paper characterizes the reachability and safety of SHSs as a viscosity solution of a system of coupled HJB equations and employs a numerical method based on discrete approximations for verification of reachability properties. The main advantage of the approach is that it guarantees the convergence of the solution based on the discrete approximation to the solution of the original problem. The approach can be extended to controlled SHSs by imposing appropriate conditions for admissible controls. Convergence of the discrete approximation methods can be investigated using relaxed controls. Characterization of error bounds as a function of the approximation parameter is a challenging problem under investigation. Another fundamental challenge is to develop scalable numerical methods that can be applied to large systems. Toward this goal, we are currently investigating methods based on variable

resolution grids and parallel algorithms as well as methods based on value function approximation.

REFERENCES

[1] D. Kozen, "A probabilistic PDL," *J. Comput. Syst. Sci.*, vol. 30, no. 2, pp. 162–178, Apr. 1985.

[2] L. de Alfaro, T. Henzinger, and R. Majumdar, "Discounting the future in systems theory," in *Proc. ICALP*, J. Baeten, J. Lenstra, J. Parrow, and G. Woeginger, Eds. Springer-Verlag, 2003, vol. 2719, pp. 1022–1037.

[3] H. Kushner and P. Dupuis, *Numerical Methods for Stochastic Control Problems in Continuous Time*. New York: Springer-Verlag, 2001.

[4] W. Fleming and H. Soner, *Controlled Markov Processes and Viscosity Solutions*. New York: Springer-Verlag, 1993.

[5] A. Fehnker and F. Ivančić, "Benchmarks for hybrid systems verification," in *Proc. HSCC*, R. Alur and G. Pappas, Eds. Springer-Verlag, 2004, vol. 2993, pp. 326–341.

[6] X. Koutsoukos and D. Riley, "Computational methods for reachability analysis of stochastic hybrid systems," in *Proc. HSCC*, J. Hespanha and A. Tiwari, Eds. Springer-Verlag, 2006, vol. 3927, pp. 377–391.

[7] M. Bujorianu and J. Lygeros, "General stochastic hybrid systems: Modelling and optimal control," in *Proc. 43rd IEEE Conf. Decision Control*, Dec. 2004, pp. 1872–1877.

[8] J. Hu, J. Lygeros, and S. Sastry, "Towards a theory of stochastic hybrid systems," in *Proc. HSCC*, N. Lynch and B. Krogh, Eds. Springer-Verlag, 2000, vol. 1790, pp. 160–173.

[9] J. Hespanha, "Stochastic hybrid systems: Application to communication networks," in *Proc. HSCC*, R. Alur and G. Pappas, Eds. Springer-Verlag, 2004, vol. 2993, pp. 387–401.

[10] M. Bernadskiy, R. Sharykin, and R. Alur, "Structured modeling of concurrent stochastic hybrid systems," in *Proc. FORMATS/FTRTFT*, Y. Lakhnech and S. Yovine, Eds. Springer-Verlag, 2004, vol. 3253, pp. 309–324.

[11] S. Amin, A. Abate, M. Prandini, J. Lygeros, and S. Sastry, "Reachability analysis for controlled discrete time stochastic hybrid systems," in *Proc. HSCC*, J. Hespanha and A. Tiwari, Eds. Springer-Verlag, 2006, vol. 3927, pp. 49–63.

[12] M. Bujorianu, "Extended stochastic hybrid systems and their reachability problem," in *Proc. HSCC*, R. Alur and G. Pappas, Eds. Springer-Verlag, 2004, vol. 2993, pp. 234–249.

[13] S. Prajna, A. Jadbabaie, and G. Pappas, "Stochastic safety verification using barrier certificates," in *Proc. 43rd IEEE Conf. Decision Control*, Dec. 2004, pp. 929–934.

[14] M. Davis, *Markov Models and Optimization*. London, U.K.: Chapman & Hall, 1993.

[15] M. Bujorianu and J. Lygeros, "Reachability questions in piecewise deterministic Markov processes," in *Proc. HSCC*, O. Maler and A. Pnueli, Eds. Springer-Verlag, 2003, vol. 2623, pp. 126–140.

[16] S. Strubbe, A. Julius, and A. van der Schaft, "Communicating piecewise deterministic Markov processes," in *Proc. IFAC Conf. ADHS*, Jun. 2003, pp. 349–354.

[17] 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*, W. McEneaney, G. Yin, and Q. Zhang, Eds. Boston, MA: Birkhäuser, 1999, pp. 249–268.

[18] J. Lugeros, "On reachability and minimum cost optimal control," *Automatica*, vol. 40, no. 6, pp. 917–927, Jun. 2004.

[19] I. Mitchell, A. Bayen, and C. Tomlin, "A time-dependent Hamilton–Jacobi formulation of reachable sets for continuous dynamic games," *IEEE Trans. Autom. Control*, vol. 50, no. 7, pp. 947–957, Jul. 2005.

[20] I. Mitchell and J. Templeton, "A toolbox of Hamilton-Jacobi solvers for analysis of nondeterministic continuous and hybrid systems," in *Proc. HSCC*, M. Morari and L. Thiele, Eds. Springer-Verlag, 2005, vol. 3414, pp. 480–494.

[21] M. Puterman, *Markov Decision Processes*. Hoboken, NJ: Wiley, 2005.

[22] C. Courcoubetis and M. Yannakakis, "The complexity of probabilistic verification," *J. ACM*, vol. 42, no. 4, pp. 857–907, Jul. 1995.

[23] L. de Alfaro, "Computing minimum and maximum reachability times in probabilistic systems," in *Proc. CONCUR*, J. Baeten and S. Mauw, Eds. Springer-Verlag, 1999, vol. 1664, pp. 66–81.

[24] X. Koutsoukos, "Optimal control of stochastic hybrid systems based on locally consistent Markov decision processes," *Int. J. Hybrid Syst.*, vol. 4, pp. 301–318, 2004.

[25] J. Hu, M. Prandini, and S. Sastry, "Probabilistic safety analysis in three dimensional aircraft flight," in *Proc. 42nd IEEE Conf. Decision Control*, Maui, HI, Dec. 2003, pp. 5335–5340.

[26] C. Tomlin, I. Mitchell, A. Bayen, and M. Oishi, "Computational techniques for the verification of hybrid systems," *Proc. IEEE*, vol. 91, no. 7, pp. 986–1001, Jul. 2003.

[27] E. Asarin, O. Bournez, T. Dang, and O. Maler, "Approximate reachability analysis of piecewise-linear dynamical systems," in *Proc. HSCC*, N. Lynch and B. Krogh, Eds. Springer-Verlag, 2000, vol. 1790, pp. 21–31.

[28] A. Chutinan and B. Krogh, "Computational techniques for hybrid system verification," *IEEE Trans. Autom. Control*, vol. 48, no. 1, pp. 64–75, Jan. 2003.

[29] O. Botchkarev and S. Tripakis, "Verification of hybrid systems with linear differential inclusions using ellipsoidal approximations," in *Proc. HSCC*, N. Lynch and B. Krogh, Eds. Springer-Verlag, 2000, vol. 1790, pp. 73–88.

[30] R. Alur, T. Dang, J. Esposito, Y. Hur, F. Ivančić, V. Kumar, I. Lee, P. Mishra, G. Pappas, and O. Sokolsky, "Hierarchical modeling and analysis of embedded systems," *Proc. IEEE*, vol. 91, no. 1, pp. 11–28, Jan. 2003.

[31] D. Riley, X. Koutsoukos, and K. Riley, "Safety analysis of sugar cataract development using stochastic hybrid systems," in *Proc. HSCC*, A. Bemporad, A. Bicchi, and G. Buttazzo, Eds. Springer-Verlag, 2007, vol. 4416, pp. 758–761.

[32] D. Bertsekas and J. Tsitsiklis, *Parallel and Distributed Computation: Numerical Methods*. Englewood Cliffs, NJ: Prentice-Hall, 1989.

[33] A. Jazwinski, *Stochastic Processes and Filtering Theory*. New York: Academic, 1970.

[34] D. Bertsekas and S. Shreve, *Stochastic Optimal Control: The Discrete Time Case*. New York: Academic, 1978.

[35] P. Tseng, "Solving H-horizon, stationary Markov decision problems in time proportional to log(H)," *Oper. Res. Lett.*, vol. 9, no. 5, pp. 287–297, Sep. 1990.

Xenofon D. Koutsoukos (S'96–M'00–SM'08) received the Diploma in electrical and computer engineering from the National Technical University of Athens, Athens, Greece, in 1993 and the M.S. degree in electrical engineering and applied mathematics and the Ph.D. degree in electrical engineering from the University of Notre Dame, Notre Dame, IN, in 1998 and 2000, respectively.

From 2000 to 2002, he was a member of Research Staff with the Xerox Palo Alto Research Center, Palo Alto, CA, working in the Embedded Collaborative Computing Area. Since 2002, he has been with the Department of Electrical Engineering and Computer Science, Vanderbilt University, Nashville, TN, where he is currently an Assistant Professor and a Senior Research Scientist in the Institute for Software Integrated Systems. He has authored or coauthored more than 70 technical publications and is the holder of three U.S. patents. His research interests include hybrid systems, real-time embedded systems, and sensor networks. He currently serves as Associate Editor for the *ACM Transactions on Sensor Networks* and for Modelling Simulation Practice and Theory.

Dr. Koutsoukos is a member of the Association for Computing Machinery (ACM). He was the recipient of the National Science Foundation CAREER Award in 2004.

Derek Riley received the B.A. degrees in computer science and math from Wartburg College, Waverly, IA, in 2004 and the M.S. degree in computer science from Vanderbilt University, Nashville, TN, in 2006. He is currently working toward the Ph.D. degree in computer science at Vanderbilt University.

Since June 2005, he has been a Graduate Research Assistant with the Institute for Software Integrated Systems, Department of Electrical Engineering and Computer Science, Vanderbilt University. His research interests include modeling and verification of stochastic hybrid systems and high-performance computing.

Mr. Riley was the recipient of the Outstanding Senior Awards in computer science and math at Wartburg College and the Vanderbilt IBM Graduate Fellowship Award.