Approximate Abstractions of Stochastic Hybrid Systems

Manuela L. Bujorianu, Marius C. Bujorianu, [*]
Henk A.P. Blom [**]

[*] *Faculty of Computer Science, Unversity of Twente, The Netherlands*
(e-mail: manuela@ ewi.utwente.nl)
[**] *National Aerospace Laboratory - NLR, Amsterdam, The Netherlands*
(e-mail: blom@nlr.nl)

Abstract: This paper considers the issue of developing approximate abstractions of stochastic hybrid systems. The stochastic continuous behaviour breaks many essential properties of hybrid automata. Our approach departs from the progress in stochastic reachability analysis and Markov chain approximations. For this purpose we have to introduce a new approximation scheme and look for a suitable metric. We construct an exponential timestepping approximation scheme for general Markov processes. This approximation scheme relies on the complex space of system trajectories involving a sensible choice of the metric. Fortunately, the Skorokhod metric is sly enough to overcome the problems. Keywords: stochastic hybrid systems, approximations, step processes, approximate abstraction, model checking.

1. INTRODUCTION

Stochastic hybrid systems (SHS) can be thought of as randomisation of the hybrid automata models. This perspective is very tempting especially because it makes easy to classify systems. For e.g., by quantifying probabilistically the discrete transition only, one obtains the well-known model of Piecewise Deterministic Markov Process (PDMP) Davis [1993]. By symmetry, an interesting class of systems is obtained randomising the continuous evolutions only: a discrete automaton controls a set of random dynamical systems. Unfortunately, this nice system based view is very misleading. The researcher in hybrid system would be tempted to think that the specification and verification techniques used in the deterministic case might be conveniently extended to the stochastic case. This viewpoint is particularly encouraged by the success of the probabilistic formal methods in the discrete case. The ruthless reality is that when the continuous evolutions are randomised, the useful properties of hybrid automata are lost. Consequently, some metrics and temporal logics defined for deterministic hybrid systems can not be anymore defined for the stochastic versions.

However, the stochastic verification must follow the same strategy like for deterministic hybrid systems via discrete approximations (or abstractions) of the given system. Again, there are difficulties in extending the probabilistic formal methods from discrete to the continuous case. One important obstacle is given by the missing concept of next state in the continuous case.

Even in the case of PDMP the dependence of the jump probabilities on the continuous evolution changes significantly the nature of the model.

The pioneering steps towards formal verification of SHS have been made, in the recent years, by several approaches in stochastic reachability analysis (SRA) Prandini and Hu [2006]. The SRA objective represents, in the stochastic models of large computer networks, a measure of a peformability, and its upper bounds estimations constitute formal specifications. In this interpretation, the SRA methods can be thought of as model checking of the performance properties. In Prandini and Hu [2006], the SRA is performed by approximations with Markov chains, which opens the possibility of performing model checking of performance properties using the discrete probabilistic model checking.

This paper presents further steps in the foundations of formal specification and model checking by employing methods of approximation of SHS. We depart from the previous work in approximation of SHS by Markov chains using for the first time the following important concepts: (i) step process (pure jump Markov processes) instead of Markov chains; (ii) the Skorokhod metric Ethier [1986]; (iii) exponentially distributed approximation step times.

The standard approximation techniques are developed for estimation purposes and they are based on equidistant observation times. This is convenient for mathematical proofs and for implementation, but not for modelling real life applications. In general, the observable approximant is a stochastic process with exponentially distributed sojourn times for each state.

In this work, we focus on the most basic step of investigating new approximation methods that make possible formal specification and verification of safety properties of SHS.

In section 2, we construct a general exponential timestepping approximation scheme for a very large class of Markov processes. In Section 3, we present a general model for SHS. As explained in Pola and Bujorianu [2003], it includes most of the other models of SHS as instances. In Section 4, we show the advantages for analysis, specification and verification of SHS, if we apply to SHS the approximation

scheme developed in Section 2. The paper ends with some final remarks.

2. APPROXIMATIONS OF MARKOV PROCESSES

All in all, in this section, we obtain an exponential timestepping approximation method, for strong Markov processes whose trajectories are right continuous and left limits, taking values in a complete separable metric space. We construct a sequence of Markov step processes that converges to the given process. Naturally, the metric employed in the convergence result is the Skorokhod metric. The result is natural since, it is known that each cadlag function can be approximated by piecewise constant function (Th. 6.2.2 Whitt [2002]). Therefore, one would expect to find a possibility to approximate stochastic processes with cadlag paths by step processes. Similar result has been obtained in Ma e.a. [2000], but for Hunt processes and with a completely different proof.

2.1 Motivation

In this paragraph, we derive the key ideas for defining approximate abstractions for general classes of SHS. In practice, since the trajectories of an SHS can not be described in a transitional system manner (a concept of next state is not available), to find analytical solutions for the reachability problem (i.e. to compute the reach set probabilities) is a challenging problem. A natural way to approach this problem is to find suitable abstractions of the given model such that they satisfy requirements as follows: 1. to be *observable* (transition system with an explicit next state representation), 2. to have the *Markov property* (in the model, a system is allowed to hold in state for an exponentially distributed time), 3. there is a suitable *probabilistic logic* to specify interesting system properties, 4. a concept of *accuracy* of approximation should be expressible mathematically by using specific metrics: the accuracy of approximation should be reflected in the error of approximation of the reach set probabilities.

Therefore, different methods for defining approximations/abstractions of SHS should necessarily be based on the study of the approximation schemes available for stochastic processes. The motivation of this is the fact that the trajectories of different classes of SHS make up a Markov process with a hybrid state space. Thus, when we have to approximate SHS, we may consider two approaches:

• Approximate the continuous dynamics in each mode (usually a diffusion process), keeping the SHS modes (the discrete state).

• Consider the space of trajectories and some observation times and construct some 'elementary trajectories' (step functions) which approximate the initial trajectories.

In literature, there exist two strategies to construct approximations for stochastic processes, namely approximation schemes that involve:

• an *equidistant time* discretisation of the given process and approximation stochastic differential equations (SDE) by difference equations (Euler/Taylor scheme, jump adapted schemes, the general finite difference method Kushner [1992]);

• an *exponential timestepping* discretisation and approximation of the process generator (Yosida approximations Ethier [1986].

Verification methods for SHS using Markov chain approximations have been developed by Krystul and Bagchi in Bagchi [2004], Krystul and Blom in Blom [2005] and Prandini and Hu in Prandini and Hu [2006]. One important remark about these approaches is that all of them use the Euler scheme approximation for a particular class of SHS.

We develop an exponential timestepping approximation for a general class of Markov processes, which includes, as a subclass, the stochastic processes that appear in the behaviour description of SHS. For a given process, we use this (Poisson like) scheme to construct a sequence of step processes or jump processes in the terminology of Davis [1993], which converges in the Skorokhod topology Ethier [1986] to the initial process. In this case, the accuracy of approximation is described by the Skorokhod metric, i.e. the paths of the given process and the paths of approximants can be transformed into each other by small deformations of space when the time has to be considered close. For any $\varepsilon \in (0,1)$ and $\delta > 0$ we can choose an element of this sequence such that the probability measure of those paths that are 'far' from those of the initial process (i.e. the Skorokhod distance between them is bigger than δ) is less than ε. This will be an $\varepsilon - \delta$- *approximate abstraction* of the given process.

For the existing numerical methods, one of the most difficult tasks is the measurement of exit times, where the quantity of interest is the first time when a process reaches a given target set or exits a region. Even if the process updates are generated with good accuracy, large errors can result from the possibility that the boundary is attained during the timestep although the process is within the boundary at both the beginning and the end of timestep. Exponential time stepping algorithms have been proved to be efficient for exit time problems for stochastic differential equations because a boundary test can be performed at the end of each timestep, providing high-order convergence in numerical evaluation of mean exit times.

2.2 Background

We first fix our notations by recalling the basic definitions (strong Markov process, step process and Skorokhod topology) needed in this paper. We use the terminology of the comprehensive monograph Ethier [1986], which is one of the most complete treatise on Markov process theory.

Strong Markov Process. We fix $(\Omega, \mathcal{F})$ a measurable space. Let X be a topological Hausdorff space and assume that $\mathcal{B}$ is the Borel σ-algebra of X. Let $\mathcal{B}^b(X)$ the Banach space of all bounded, real-valued, Borel measurable functions on X with $||f|| = \sup_{x \in X} |f(x)|$.

Let $M = (\Omega, \mathcal{F}, \mathcal{F}_t, (x_t)_{t \geq 0}, (P_x)_{x \in X})$ be a Markov process with the state space $(X, \mathcal{B})$. The elements $\mathcal{F}_t$, P_x are standard defined as any textbook Ethier [1986]. A Markov process M is called *strong Markov* if the Markov property holds for every stopping time w.r.t. its natural filtration

$(\mathcal{F}_t)$. For detailed definitions consult Ethier [1986]. In this paper, we will make use of the following parametrizations of M:

The *operator semigroup* is $\mathcal{P} = (P_t)_{t>0}$: $P_t f(x) = \int f(y) p_t(x, dy) = E_x f(x_t), f \in \mathcal{B}^b(X), \forall x \in X$; where E_x is the expectation w.r.t. P_x, and p_t is the transition function of M. The operator semigroup $(P_t)_{t>0}$ is, in fact, the collection of all first order moments, which can be associated with the family of random variables $\{x_t | t > 0\}$.

The *operator resolvent* $\mathcal{V} = (V_r)_{r\geq 0}$ associated with $\mathcal{P}$ is

$$V_r f(x) = \int_0^\infty e^{-rt} P_t f(x) dt, f \in \mathcal{B}^b(X), x \in X. \qquad (1)$$

The operator resolvent $(V_r)_{r\geq 0}$ is the *Laplace transform* of the semigroup.

The infinitesimal generator L is the derivative of P_t at $t = 0$. Let $D(L) \subset \mathcal{B}^b(X)$ be the set of functions f for which the limit $\lim_{t\searrow 0} \frac{1}{t}(P_t f - f)$ exists and denote this limit Lf.

Skorokhod Topology. In this paragraph (X, d) is a fixed complete separable metric space. We consider the set $D_X[0, \infty)$ of all paths $x : [0, \infty) \to X$ that are right continuous and have left limits (i.e. the space of all *cadlag*[1] *functions* from $[0, \infty)$ to X). Such functions are known also as *Skorokhod functions*. A topological structure (topology) on the space $D_X[0, \infty)$ has been introduced by Skorokhod as an alternative to the topology of uniform convergence in order to study the *convergence in distribution* of stochastic processes with jumps Whitt [2002]. This topology is generated by a metric related to d (see Ethier [1986], III).

Skorokhod has given a Polish topology on $D_X[0, \infty)$. It rests on the idea that temporal as well spatial measurements are subject to errors, and that paths that can be transformed into each other by small deformations of space and time should be considered close.

The space $D_X[0, \infty)$ is separable and complete under the metric d_S (the Skorokhod metric). The Polish topology induced by d_S is called the *Skorokhod topology on* $D_X[0, \infty)$ and coincides on $C_X[0, \infty)$ (the space of continuous functions on $[0, \infty)$ with values in X) with the topology of uniform convergence on bounded intervals.

Step Processes. For the formal definition of *Markov step processes* (or pure jump process) we refer to Davis [1993]. In an equivalent manner to define a step process is to start with a counting process $(\theta_t)_{t\geq 0}$ (e.g. Poisson process) with the intensity λ, and a Markov chain (X_n) with the transition kernel μ. Then, the step process is defined as $x_t := X_{\theta_t}$. This description can be used to simulate a step process:

1) $x = X_0$, $t = 0$;

2) Generate a random time interval S_n exponentially distributed with the rate $\lambda(x, t)$;

3) Increase time $t := t + S_n$;

4) Jump $x \to y$, where the post jump location is given the stochastic kernel $\mu(x, t)$; If $t < t_{\max}$ go back to step 2.

2.3 Approximation Construction

In this section we construct an exponentially timestepping approximation scheme (ETAS) for strong Markov processes with cadlag property.

Hypotheses. Let X be a Polish space. We consider the measurable space $(X, \mathcal{B}(X))$, where $\mathcal{B}(X)$ or $\mathcal{B}$ is the Borel σ-algebra of X (i.e. the σ-algebra generated by the open sets).

More generally, we can consider that X is a Borel space, i.e. it is homeomorphic to a Borel subset of a complete separable space. The concept of Borel space is quite broad, containing any "reasonable" subset of n-dimensional Euclidean space. Let us consider a strong Markov process $M = (\Omega, \mathcal{F}, \mathcal{F}_t, x_t, P_x)$. Suppose that M has the cadlag property and the state space $(X, \mathcal{B})$. Let d be a compatible metric on X. We adjoin an extra point Δ (the cemetery) to X as an isolated point, $X_\Delta = X \cup \{\Delta\}$ in order to capture the situation when the transition probability $p_t(x, X) < 1$, i.e. the process escapes to and is trapped in a point outside of its state space.

Let $(P_t)_{t>0}$ (resp. $(V_r)_{r\geq 0}$) be its operator semigroup (resp. operator resolvent (1)).

Ingredients. Fix $x \in X$; in the following discussion, P_x is the law of M under the initial condition $x_0 = x$. In order to construct the sequence of jump processes that approximate M, we need the following ingredients:

1. A sequence of Markov chains (α^n). Each $\alpha^n = (\alpha^n_k)_{k=0,1,2,\ldots}$ is a Markov chain on X_Δ with some initial distribution ν and the (homogeneous) transition function, K_n given by

$$K_n(x, dy) := nV_n(x, dy) \qquad (2)$$

where V_n is the stochastic kernel computed from formula (1), i.e. is the Laplace transform of the transition probability function of M for $r = n$.

2. A sequence of Poisson processes (θ^n). Each $\theta^n = (\theta^n_t)_{t\geq 0}$ is a Poisson process[2] with the parameter n, independent of α^n.

These ingredients will help us to define, for each $n \geq 1$, a *continuous-time (regular) Markov step* process on X_Δ by

$$\rho^n_t := \alpha^n_{\theta^n_t}, t \geq 0. \qquad (3)$$

whose embedded marked point process has the intensity equal to n and state space X_Δ. This means that the jump times of the process (ρ^n_t) are given by the arrival times of the Poisson process (θ^n_t) and its values between jumps are provided by the Markov chain (α^n_k).

The reader might be wondering at this point why we focus hereafter on the continuous-time process (ρ^n_t), rather than on the apparently simpler Markov chain (α^n_k). The motivation is twofold: (i) We have to make transition

[1] This is an acronym for the French phrase "continue à droite avec limites à gauche" meaning "continuous on the right with left limits".

[2] i.e. $P(\theta^n_t = k) = \exp(-nt)\frac{(nt)^k}{k!}$

from discrete time to continuous time at some place in the argument, and from the probabilistic viewpoint it is convenient to do this at the very beginning. For e.g., it is not possible to use the Skorokhod metric between the trajectories of the initial process and the traces of discrete time Markov chain. (ii) There exist many models where we want the jump rate to vary according to some process parameters and the above construction is suitable for this.

Note that $K_n(x,\cdot)$, given by (2), can be thought of as the P_x-distribution of x_T, where T is random time independent of M and exponentially distributed with rate n Kallenberg [1997]. The kernel V_n can be computed using the generator L of the process M by formula

$$V_n := (nI - L)^{-1}, n \geq 1. \quad (4)$$

where I is the identity operator Ethier [1986]. Moreover, V_n is *potential kernel* of the process M killed with the exponential rate n Kallenberg [1997].

Convergence. The following theorem shows that the above sequence of step processes converges in the Skorokhod topology and consequently it converges weakly (in distribution) to the initial Markov process.

Theorem 1. If $\alpha_0^n = x$, then the sequence $\{\rho^n\}_{n\geq 1}$ of step processes converges weakly to M (under P_x) as $n \to \infty$.

2.4 Approximate Equivalence/Abstraction

For the purposes of this paper, we have to make clear the concept of Markov process *approximant* with the cadlag property. For a given Markov process, the transition probabilities of an approximant do not match exactly the transition probabilities of the initial process. Thus we need to define an *approximate equivalence* for Markov processes.

Definition 1. The processes M and M' are ε−δ-approximate equivalent ($1 > \varepsilon > 0$, $\delta > 0$) if and only for all $x \in X$

$$P_x\{\omega \in \Omega : d_{[0,u]}(x_t(\omega), x'_t(\omega)) > \delta\} < \varepsilon, \forall u > 0 \quad (5)$$

where $d_{[0,u]}$ is the Skorokhod distance in the path space $D_X[0,u]$.

The process M' is called $\varepsilon - \delta$-*approximant* ($1 > \varepsilon > 0$, $\delta > 0$) of M, or viceversa.

Then, we introduce the concept $\varepsilon - \delta$-approximate abstraction for continuous time continuous space Markov processes with cadlag property.

Definition 2. The process M' is called $\varepsilon - \delta$-*approximate abstraction* ($1 > \varepsilon > 0$, $\delta > 0$) of M if M' is a Markov step process and is an $\varepsilon - \delta$-*approximant* of M.

Proposition 2. For any $\varepsilon \in (0,1)$, $\delta > 0$ there exists a countable sequence of $\varepsilon - \delta$-approximate abstractions of M.

3. STOCHASTIC HYBRID SYSTEMS

General Stochastic Hybrid systems (GSHS) are a class of non-linear stochastic continuous-time hybrid dynamical systems. The model is rather general, since it encompasses most of the interesting models for SHS existing in the literature Pola and Bujorianu [2003]. The specific features of GSHS, like its componentwise diffusion structure or its infinitesimal generator Bujorianu and Lygeros [2006] will not be explicitly used in this paper, but a numerical approach based on the theory presented here will heavily make use of these characteristics.

In the following, the syntax and the semantics of GSHS are briefly presented and also some mathematical properties are pointed. As usual, the GSHS hybrid state space is $X := \bigcup_{i\in Q}\{i\} \times X^i$ and the hybrid state $x := (i, z^i) \in X$ (i is the discrete state belonging to a countable set Q and z^i is the continuous state evolving in some Euclidean open sets X^i). It is known that X can be endowed with a metric d whose restriction to any component X^i is equivalent to the usual component metric Davis [1993]. Then $(X, \mathcal{B}(X))$ is a Borel space [3], where $\mathcal{B}(X)$ is the Borel σ-algebra of X. Note that Borel space means that it is homeomorphic to a Borel subset of a complete separable space. The concept of Borel space is quite broad, containing any "reasonable" subset of the n-dimensional Euclidean space.

A GSHS is defined as a stochastic hybrid automaton $H = ((Q, \kappa, \mathcal{X}), b, \sigma, Init, \lambda, R)$ Bujorianu and Lygeros [2006]. The executions of a GSHS can be described as follows: start with an initial point $x_0 \in X^q$ according to $Init$, follow a solution of the SDE (with the parameters given by b and σ) associated to X^q, jump when this trajectory hits the boundary or according with the transition rate λ (the jump time is the minimum of the boundary hitting time and the time, which is exponentially distributed with the transition rate λ). For each initial condition $x \in \bigcup_{j\in Q} X^j$, the possible trajectories (executions of H) starting from x, form a stochastic process.

Let us consider $M = (\Omega, \mathcal{F}, \mathcal{F}_t, x_t, P_x)$, the realization or behaviour of H (the set of all executions of H). Under standard assumptions Bujorianu and Lygeros [2006] on the parameters of H: (i) assumption on the diffusion coefficients, which ensures that for any $i \in Q$, the existence and uniqueness of the solution of the SDE corresponding to each mode; (ii) assumption about non-Zeno executions; (iii) assumption about the transition measure the transition rate function; M can be viewed as a family of Markov processes.

It was proved that the realization M of a GSHS, H, is a Borel right process Bujorianu and Lygeros [2006], i.e. it belongs to a special class of strong Markov processes. Moreover, it was proved that M has right-continuous left-limited sample paths (*cadlag property*) Bujorianu and Lygeros [2006]. Then the realizations of a GSHS make up a family of Markov processes $M = (\Omega, \mathcal{F}, \mathcal{F}_t, x_t, P_x)$ on $\Omega = D_X[0,\infty)$ Bujorianu and Lygeros [2006] [4], which can be thought of as a Markov process in a general setting Davis [1993].

4. APPROXIMATIONS/ABSTRACTIONS OF SHS

In this section, we want to justify that the ETAS developed in Section 2 could be very useful in the SHS analysis, safety property specification and verification.

[3] Note that for the majority of the stochastic hybrid system models the state space is a Borel space Pola and Bujorianu [2003].

[4] Each trajectory, which is a cadlag function, is an elementary event of the probability space.

4.1 SHS Approximation

The main result of the Section 2, Th.1, states that for every strong Markov process with cadlag property defined on a Polish space can be approximated in the Skorokhod topology by a suitable sequence of Markov step processes.

Let us briefly remind some SHS features that make ETAS suitable for SHS: (a) The state space is a Borel space, which can be embedded in a Polish space. (b) The realizations are cadlags, then they belong to a Skorokhod space. The ETAS convergence uses the Skorokhod metric, which is the most suitable metric for cadlags. This metric can 'detect jumps', i.e. a sequence of functions with jumps cannot converge to a continuous function and a sequence of continuous functions does not approximate a function with jumps Whitt [2002]. Then, SHS will be approximated by other much simpler SHS, whose trajectories are piecewise constant. (c) In the most cases, the expression of the infinitesimal generator and the martingale characterization are known Bujorianu and Lygeros [2006]. Therefore, in the ETAS, the computation of the Markov chain transition kernel, expressed using the resolvent operator or the generator (see (2) and (4)), is feasible and can be numerically done.

At this point, we have to explain how the hybrid structure of an SHS dynamics is considered in ETAS. For each $\omega \in \Omega$, a hybrid trajectory $x_t(\omega) = (q_t(\omega), z_t(\omega))$ of an SHS, H, can be thought of as the union 'diffusion components' $\{z_t(\omega) | T_k(\omega) \leq t < T_{k+1}(\omega),\ k = 1, 2, ...\}$ where $T_1 < T_2 < ...$ represent the jump times of H. Each component is provided with the label $q_{T_k(\omega)}(\omega)$ since $q_t(\omega)$ is constant in the random time interval $[T_k(\omega), T_{k+1}(\omega))$. Then, a cadlag trajectory of H is implicitly carrying the hybrid dynamics structure. In the ETAS, we do <u>not</u> interpolate the Poisson times of step processes considered there with the jumping times of H. The reason for not doing this is that the latter jumping times can not be explicitly computed since a jumping time might be the first boundary hitting time of some diffusion process or some random time exponentially distributed with a rate depending on the piece of diffusion trajectory covered until that moment.

In the ETAS, proposed in this paper, the trajectories of the system are considered 'first class citizens' and the methodology is heavily based on the use of a metric defined on the space of all possible trajectories. Due to the complexity of the hybrid trajectories, it was proved, even in the deterministic case, that a hybrid system H_1 is an *approximate abstraction or an approximation* of the hybrid system H_2 if for every trajectory of H_2 there exists a trajectory of H_1 such that the distance between these trajectories is small enough. Therefore, we considere the ETAS to be the most suitable procedure to provide for a given SHS, H, an approximate abstraction.

4.2 SHS Approximate Abstractions

Let H and H' be two GSHS.

Assumption 1. Suppose that the two GSHS H and H' have the state space X.

This assumption is to ease our work. One can think at the common state space as the direct sum of the state spaces associated to the two SHS.

We assume that H and H' satisfy the standard assumptions from the section 3. We suppose that X is a Borel space. Let d be a compatible metric on X. Then, we consider their realizations $M = (\Omega, \mathcal{F}, \mathcal{F}_t, x_t, P_x)$ and $M' = (\Omega', \mathcal{F}', \mathcal{F}'_t, x'_t, P_x)$. Since we have supposed that H and H' have the same state space, then $\Omega = \Omega' = D_X[0, \infty)$.

For the realization of a GSHS, we are interested in those $\varepsilon - \delta$ -approximants, which corresponds to simpler GSHS whose continuous dynamics is piecewise constant. More precise, we are looking for $\varepsilon - \delta$-approximants which are Markov step processes.

Definition 3. The GSHS H' is called $\varepsilon - \delta$-approximate abstraction $(1 > \varepsilon > 0,\ \delta > 0)$ of H if its realization M' is an ε-approximate abstraction of the realization M of H.

For any $\varepsilon \in (0, 1)$, $\delta > 0$, Proposition 2 states that for any GSHS, under the standard assumptions, there exists always an $\varepsilon - \delta$-approximate abstraction H' of H, close enough to H (closeness measured in terms of the distance between the trajectories). Intuitively, in the ETAS, the realization of H' is one of the step processes whose trajectories are enough close to the trajectories of H and the jump times are given by a Poisson process with intensity $n \in \mathbb{N}$, where n is big enough. This means that the sojourn times of M' (the realization of H') in each state are very small and at some level of approximation M' can be thought of as an marked point process $(T'_k, x'_{T'_k})$, i.e. a sequence of timepoints (T'_k) marking the occurrence of events $(x'_{T'_k})$ Kallenberg [1997]. Therefore, in applications, one might work for simplicity with the Markov chain $(x'_{T'_k})$ associated to M' (see subsection 2.2).

In the following subsection, we will sketch how to employ the concept of approximate abstraction in the SHS verification. More, this concept makes available the possibility to use probabilistic logics to specify different properties of the initial SHS.

4.3 Applications

SHS Verification using Approximations/Abstractions

In this subsection, we conceptually define the model checking problem in the context of SHS and show how the ETAS can be fruitfully applied in order to ease the SHS verification problem. Our proofs are based on the characterization of the weak convergence of Markov processes in terms of the generators/ martingales Ethier [1986].

Consider a strong Markov process $M = (\Omega, \mathcal{F}, \mathcal{F}_t, x_t, P_x)$ with cadlag trajectories, which constitutes the evolution of a stochastic hybrid system with the state space X (equipped with the metric d and Borel σ-algebra $\mathcal{B}(X)$). Mathematically, this might be an element of a particular class of diffusions Prandini and Hu [2006], diffusions with hybrid jumps Blom [2003], switching diffusions, piecewise deterministic Markov processes (see Pola and Bujorianu [2003] for an overview).

To address the stochastic reachability problem, assume that we have given a set $A \in \mathcal{B}(X)$ and a (finite or infinite) time horizon $T \in [0, \infty]$. Let us to define:

$$Reach_T(A) = \{\omega \in \Omega \mid \exists t \in \mathcal{T} : x_t(\omega) \in A\}. \quad (6)$$

where $\mathcal{T} = [0, T]$ or $[0, \infty)$, depending on the time horizon T. The problem consists of determining the probabilities of such a set.

We define the probabilities of reach events as $P[Reach_T(A)]$, where P is a probability, which can be chosen to be P_x (if we want to consider the trajectories, which start in x).

On the other hand, these probabilities can be described as $P_x(T_A \leq T)$ or $P_x(T_A < \infty)$, where

$$T_A = \inf\{t > 0 | x_t \in A\} \quad (7)$$

is the first hitting time of A.

The first approach to compute the reach set probabilities is 'to look at the errors'. The accuracy of an approximation (ρ_t) (understood as a Markov process with the same state space) for the initial model w.r.t. the model checking problem can be expressed mathematically asking that the following error to be 'small enough'

$$Err(T, A, (x_t), (\rho_t)) = \mid E_x 1_{[T_A \leq T]} - E_x 1_{[T'_A \leq T]} \mid \quad (8)$$

where E_x is the expectation w.r.t. P_x, T'_A is the first hitting time of A w.r.t. (ρ_t).

Approximate abstractions can be very useful in order to get various upper bounds for reach set probabilities. Suppose now that M' a step process, which is an $\varepsilon - \delta$ - approximate abstraction of M. The reach event $Reach'_T(A)$ for M' is given as in (6), with x_t replaced by x'_t. This means that $\omega \in Reach'_T(A)$ if and only if there exists $t_0 \in [0, T]$ such that $x'_{t_0}(\omega) \in A$. Let us define the vicinity closure of A with respect to δ and d as

$$cl_\delta(A) := \{x \in X \mid \exists y \in A : d(x, y) \leq \delta\}.$$

Clearly $cl_\delta(A) \in \mathcal{B}(X)$ since d is a continuous map in both variables.

Proposition 3. For all $A \in \mathcal{B}(X)$, we have:

$$P_x[Reach_T(A)] \leq P_x[Reach'_T(cl_\delta(A))] + \varepsilon.$$

Another approach to the reachability problem is to look at the mean of the first hitting time of the target set A (formula (7)). When A is an unsafe set, the quantities of interest are the lower bounds on the expected value of this hitting time, since these bounds provide a degree of assurance against catastrophic failure. Dually, the mean of the first exit time from a safe domain provides a measure of its stability. It also measures the rate of transition from the domain it exits. The following result (see the proof in Appendix) shows that the expectation of the hitting time T_A of an SHS, H, can be approximated with the analogous expectation of an approximate abstraction of H.

Proposition 4. If (ρ_t^n) is a sequence of step processes given by ETAS for M, then for each $x \in X$ and $A \in \mathcal{B}(X)$ $E_x(\tau_A^n) \to E_x(T_A)$, as $n \to \infty$where, for each $n \geq 1$, τ_A^n is the first hitting time of A corresponding to $(\rho_t^n)_{t \geq 0}$.

5. FINAL REMARKS

In this paper, we focus on the issue of approximate abstractions for stochastic hybrid systems. This constitutes a fundamental issue in safety verification and it was approached by many authors from different perspectives. Due to room limitations, we hace cited only those contributions which are strictly related to our work. The importance of this issue comes also from the wide range of SHS applications that span from medicine to wireless communication, computer networks, air traffic control, etc.

The main contribution consists of an approximation technique using step Markov processes. These processes constitute the realizations of the simplest SHS. Moreover, Markov chains can be easily embedded in such processes. This technique is realistic and adapted to real life phenomena because of its exponentially distributed time stepping.

In a following paper, we will apply this approximation method for formal specification of safety properties using the continuous stochastic logic and develop a formal technique for model checking.

ACKNOWLEDGEMENTS

This work was partially supported by the NWO project AiSHA.

REFERENCES

H.A.P. Blom and J. Lygeros. Stochastic hybrid systems: theory and safety critical applications. Springer Verlag LNCIS 337, 2006.

H.A.P. Blom. Stochastic hybrid processes with hybrid jumps. Proc. IFAC Conf. ADHS, pages 361–365, 2003.

M.L. Bujorianu and J. Lygeros Lygeros. Towards modelling of general stochastic hybrid systems. In Blom and Lygeros [2006], pages 3–30, 2006.

M.H.A. Davis. Markov models and optimization. Chapman Hall , 1993.

S.N. Ethier and T.G. Kurtz. Markov processes: characterization and convergence. John Wiley, 1986.

W. Kallenberg. Foundations of modern probability. Springer Verlag, 1997.

H.J. Kushner and P. Dupuis. Numerical methods for stochastic control problems in continuous time. Springer Verlag, 1992.

J. Krystul and A. Bagchi. Approximations of first passage times of switching diffusion. *Proc. MTNS*, 2004.

J. Krystul and H.A. Blom. Sequential Monte-Carlo simulation of rare event probability in stochastic hybrid systems. *Proc. 16th IFAC World Congres*, 2005.

Z.M. Ma, M. Rockner, W. Sun. Approximate of Hunt processes by multivariate Poisson processes. *Acta Applicandae Mathematicae*, 63:233–243, 2000.

G. Pola, M.L. Bujorianu, J. Lygeros, and M. Di Benedetto. Stochastic hybrid models: an overview with applications to air traffic management. *Proc. IFAC Conf. ADHS*, Elsevier Press, pages 45–50, 2003.

M. Prandini and J. Hu. A stochastic approximation method for reachability computation. In Blom and Lygeros [2006], pages 107–139, 2006.

W. Whitt. Internet supplement to stochastic-process limits: an introduction to stochastics process and their application to queues. 2002.