State constrained reachability for stochastic hybrid systems

Bujorianu, M.L. and Bujorianu, M.C.

2009

ISSN 1749-9097

State Constrained Reachability for Stochastic Hybrid Systems

Manuela L. Bujorianu * **Marius C. Bujorianu** **

* *University of Manchester, School of Mathematics, Alan Turing Building, Oxford Road, Manchester M13 9PL, UK (e-mail: Manuela.Bujorianu@manchester.ac.uk).*
** *University of Manchester, School of Mathematics, Manchester UK (e-mail: Marius.Bujorianu@manchester.ac.uk)*

Abstract: The stochastic hybrid systems constitute well established classes of realistic models of hybrid discrete/continuous dynamics subject to random perturbations, autonomous uncontrollable transitions, nondeterminism or uncertainty. Stochastic reachability analysis is a key factor in the verification and deployment of stochastic hybrid systems. The encouraging recent progress prompts us to refine the problem to cover more realistic situations. We extend the so called constrained reachability problem from the probabilistic discrete case to stochastic hybrid systems. Then we define mathematically this problem, and we obtain the reach probabilities as solutions of a boundary value problem. The last problem is well studied and numerical, even symbolic solutions exist. This characterization is useful in stochastic control, in probabilistic path planning and for nano-systems.

Keywords: stochastic hybrid systems, reachability, stochastic model checking, holistic modeling, interdisciplinary verification, aerospace and nano-engineering.

1. INTRODUCTION

Hybrid systems form a class of systems whose behaviors are characterized by a non-trivial interaction between discrete and continuous dynamics. These systems accurately model technical systems from automotive industry, aeronautics, air traffic control, robotics, and nanotechnology. Hybrid models are also used frequently in system biology and medicine, where their features make controllability and verification more difficult, mostly because of uncertainty, complex continuous dynamics, partial information, and of the so-called spontaneous transitions. In the case of open systems, the environment influence produces random evolutions increasing the complexity of verification and control problems. To address these issues, randomized models have been considered and their class is usually denoted as *stochastic hybrid systems*. Mathematically, a stochastic hybrid system can be seen as an interleaving between a finite or countable family of diffusion processes (or, sometimes, deterministic dynamical systems only) and a Markov chain. Modeling and analysis of these systems have been proved to be a very difficult task, especially from fundamental mathematical point of view. The stochastic analysis apparatus, employed to study their probabilistic properties is complex and rather difficult to manage. This study involves the ability to combine tools available for diffusion processes and jump processes, in order to characterize the executions of these systems. The switching mechanism (governed by a Markov chain in most cases) between the continuous dynamics of the modes, together with the interaction between paths and boundaries, make the studying of the stochastic processes that arise in this way very difficult and challenging.

Reachability analysis is at the heart of any verification problem for stochastic systems that discrete or continuous or hybrid discrete/continuous. The standard form of reachability analysis asks to compute/approximate the probability of all system paths that start from a given initial state and visit a target state set. In the discrete case, this problem is known as *probabilistic model checking* and there exist relatively efficient algorithms for solving it. For continuous and hybrid stochastic systems, the problem is more difficult and it is only partially solved. Theoretical solutions are based on *martingale theory* (see Bujorianu et al. [2003] and Bujorianu et al. [2007]), *Bayesian statistics* (as in Bujorianu [2005]), and *optimal control* (Bujorianu et al. [2008]). Numerical solutions are mainly based on *interactive particle systems (*Blom et al. [2007]), *Monte Carlo simulations* (Krystul et al. [2005]), *Markov chain approximations* (Prandini et al. [2006]), and *dynamic programming* (Koutsoukos et al. [2008]).

For practical reasons, the reachability analysis has got variants by inserting further conditions (constraints). The constraints can be formulated with respect to time or states see Baier et al. [2007]. For example, one can ask to estimate the probability to reach a target state set in a finite horizon time (time-constrained reachability). Relative to the states, a variant of reachability analysis may ask to evaluate the probability to reach a target set of states by avoiding a given state set (interpreted as dangerous situations). This problem is important in planning and stochastic control. From a practical site, this sort of problems arise from robotics, air traffic control, or military applications. In this paper, we formulate and investigate state-constrained reachability problem for stochastic hybrid systems. We prove that the problem is solvable. Moreover, for systems that are sufficiently "regular" (they can be approximated by diffusions), the problem can be solved symbolically or numerically.

The paper structure is as follows. In the next section, we present a model of stochastic hybrid systems and its properties. In Section 3, we present the standard stochastic reachability problem, followed by the state-constrained reachability problem. Then in Section 4, we give some characterizations of the state-constrained reachability probabilities. The paper ends with some final remarks.

2. THE COMPUTATIONAL MODEL

We adopt the *general stochastic hybrid system* model presented in Bujorianu et al. [2004] and Bujorianu et al. [2006]. In this subsection the model is described and the notation is established.

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 subset X^q of $\mathbb{R}^{d(q)}$. The hybrid state space is the set

$$X(Q, d, \mathcal{X}) = \bigcup_{i \in Q} \{i\} \times X^i$$

and

$$x = (i, z^i) \in X(Q, d, \mathcal{X})$$

is the hybrid state. The closure of the hybrid state space will be $\overline{X} = X \cup \partial X$, where $\partial X = \bigcup_{i \in Q} \{i\} \times \partial X^i$.

It is known that X can be endowed with a metric ρ whose restriction to any component X^i is equivalent to the natural Euclidean metric of this component Davis [1993]. Then $(X, \mathcal{B}(X))$ is a Borel space (homeomorphic to a Borel subset of a complete separable metric space), where $\mathcal{B}(X)$ is the Borel σ-algebra of X. Let $\mathbf{B}(X)$ be the Banach space of bounded positive measurable functions on X with the norm given by the supremum.

Definition 1. A (general) stochastic hybrid system (SHS) is a collection

$$H = ((Q, d, \mathcal{X}), b, \sigma, Init, \lambda, R)$$

where

- Q is a countable set of discrete states (modes);
- $d : Q \to \mathbb{N}$ is a map giving the dimensions of the continuous state spaces;
- $\mathcal{X} : Q \to \mathbb{R}^{d(\cdot)}$ maps each $q \in Q$ into an open subset X^q of $\mathbb{R}^{d(q)}$;
- $b : X(Q, d, \mathcal{X}) \to \mathbb{R}^{d(\cdot)}$ is a vector field;
- $\sigma : X(Q, d, \mathcal{X}) \to \mathbb{R}^{d(\cdot) \times m}$ is a $X^{(\cdot)}$-valued matrix, $m \in \mathbb{N}$,
- $Init : \mathcal{B}(X) \to [0, 1]$ is an initial probability measure on $(X, \mathcal{B}(X))$;
- $\lambda : \overline{X}(Q, d, \mathcal{X}) \to \mathbb{R}^+$ is a transition rate function;
- $R : \overline{X} \times \mathcal{B}(\overline{X}) \to [0, 1]$ is a transition measure.

A stochastic hybrid process, describing the evolution of a SHS, is built as a *Markov string* H - see Bujorianu et al. [2006] - which is obtained by the concatenation of some diffusion processes (z_t^i), $i \in Q$ together with a jumping mechanism given by a family of stopping times (S^i). Let ω_i be a diffusion trajectory, which starts in $(i, z^i) \in X$. Let $t_*(\omega_i)$ be the first hitting time of ∂X^i of the process (x_t^i). Define the function

$$F(t, \omega_i) = I_{(t < t_*(\omega_i))} \exp(-\int_0^t \lambda(i, z_s^i(\omega_i)))ds.$$

This function will be the survivor function for the stopping time S^i associated to the diffusions (z_t^i).

Definition 2. (SH process). A stochastic process

$$x_t = (q(t), z(t))$$

is called a *stochastic hybrid (SH) process* if there exists a sequence of stopping times

$$T_0 = 0 < T_1 < T_2 \leq \ldots$$

such that for each $k \in \mathbb{N}$,

- $x_0 = (q_0, z_0^{q_0})$ is a $Q \times X$-valued random variable extracted according to the probability measure $Init$;
- For $t \in [T_k, T_{k+1})$, $q_t = q_{T_k}$ is constant and $z(t)$ is a solution of the stochastic differential equation (SDE):
$$dz(t) = b(q_{T_k}, z(t))dt + \sigma(q_{T_k}, z(t))dW_t$$
where W_t is the m-dimensional standard Wiener process;
- $T_{k+1} = T_k + S^{i_k}$ where S^{i_k} is chosen according with the survivor function (2).
- The probability distribution of $x(T_{k+1})$ is governed by the law $R\left((q_{T_k}, z(T_{k+1}^-)), \cdot\right)$.

It can be shown that any SH process corresponding to an SHS H, under standard assumptions (about the diffusion coefficients, non-Zeno executions, transition measure, etc, see Bujorianu et al. [2006] for a detailed presentation) is a strong Markov process (see the definition, for example, in Ethier et al. [1986] or in Grimmett et al. [1982]). Let

$$M = (\Omega, \mathcal{F}, \mathcal{F}_t, x_t, P_x)$$

be the Markov process associated to H, where $(\Omega, \mathcal{F})$, $\{x_t\}$ is a collection of X-valued random variables, $\{\mathcal{F}_t\}$ is the natural filtration of the process (the 'history' of the process). The meaning of the elements of M can be found in any source treating continuous-parameter Markov processes (for e.g. Blumenthal et al. [1968] or Ethier et al. [1986] or Davis [1993]). We adjoin an extra point Δ (the cemetery) to X as an isolated point,

$$X_\Delta = X \cup \{\Delta\}.$$

The existence of Δ is assumed in order to have a probabilistic interpretation of

$$P_x(x_t \in X) < 1,$$

i.e. Δ is the state where the process lies when it 'dies'. Then, the 'termination time' $\zeta(\omega)$ is the random time when the process M escapes to and is trapped at Δ.

The *semigroup of operators* associated to M, denoted by

$$\mathcal{P} = (P_t)_{t>0}$$

maps $\mathbf{B}(X)$ into itself, and it is given as

$$P_t f(x) = E_x f(x_t), \forall x \in X,$$

where E_x is the expectation w.r.t. P_x.

Recall that a nonnegative function $f \in \mathbf{B}(X)$ is called *α-excessive* ($\alpha \geq 0$) (see Blumenthal et al. [1968]) if

(i) $e^{-\alpha t} P_t f \leq f$ for all $t \geq 0$, and

(ii) $e^{-\alpha t} P_t f \nearrow f$ as $t \searrow 0$.

If $\alpha = 0$, a 0-excessive function is simply called *excessive function*. Let us denote the *cone of excessive functions* by $\mathcal{E}_M$. In the theory of Markov processes, the excessive functions play the role of the superharmonic functions from the theory of partial differential equations (for e.g. a function $f \geq 0$ is superharmonic w.r.t. the Laplace operator if $\Delta f \leq 0$). Note, that the definition of excessive function can be given in terms of the *operator resolvent $\mathcal{U}$*, which is the Laplace transform of $\mathcal{P}$.

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

$$V_r f(x) = \int_0^\infty e^{-rt} P_t f(x) dt,$$

for all $f \in \mathbf{B}(X),\ x \in X$.

The infinitesimal generator $\mathcal{L}$ is the derivative of P_t at $t = 0$. Let $D(\mathcal{L}) \subset \mathcal{B}_b(X)$ be the set of functions f for which the following limit exists (denoted by $\mathcal{L}f$)

$$\lim_{t \searrow 0} \frac{1}{t}(P_t f - f)$$

The following result, proved in Bujorianu et al. [2006], is essential for the mathematical study of reachability properties.

Proposition 1. Under the standard assumptions the stochastic hybrid process M defined above is a Borel right process with the cadlag property.

Recall that a Borel right process is defined by the following properties:

(i) its sample paths $t \to x_t$ are right-continuous almost sure.

(ii) X is a separable metric space homeomorphic to a Borel subset of some compact metric space, equipped with Borel σ-algebra $\mathcal{B}(X)$ or shortly $\mathcal{B}$ (i.e. X is a Lusin state space).

(iii) The operator semigroup of M, given by (2), maps $\mathbf{B}(X)$ into itself.

(iv) If f is an α-excessive function for $\mathcal{P}$, then the sample path $t \to f(x_t(\omega))$ is a.s. right continuous (this property is equivalent with the fact M is a strong Markov process).

The sample paths of M are right continuous with left limit, i.e. are cadlags - see Bujorianu et al. [2006]. Moreover, the cadlag property added to the fact that the state space is a Lusin space, which insures a 'tightness' property of this right process, that it is concentrated on compacts.

The infinitesimal generator of an SHS is an integro-differential operator. In Bujorianu et al. [2004], it has been proved, that the extended generator of an SHS has the following expression:

$$\mathcal{L}f(x) = \mathcal{L}_{cont} f(x) + \lambda(x) \int_{X} (f(y) - f(x)) R(x, dy) \quad (1)$$

where $\mathcal{L}_{cont} f(x)$ has the standard form of the diffusion infinitesimal operator. What makes this generator different from the generator of a Feller Markov process (see Ethier et al. [1986]) is its domain that contains at least the set of second order differentiable functions that satisfy the boundary condition, as follows:

$$f(x) = \int_{\mathbb{X}} f(y) R(x, dy), x \in \partial X.$$

In the presence of forced jumps, the generator of an SHS is an operator that is difficult to deal with, since its domain does not even contain the set of all compactly supported C^∞ functions.

3. STOCHASTIC MODEL CHECKING

3.1 Stochastic Reachability

Let us consider an SH process $M = (\Omega, \mathcal{F}, \mathcal{F}_t, x_t, P_x)$ which is strong right Markov. The verification problem consists of the following *stochastic reachability problem.* Given a target set, the objective of the reachability problem is to compute the probability that the system trajectories from an arbitrary initial state will reach the target set.

Formally, given a set $A \in \mathcal{B}(X)$ and a time horizon $T > 0$, let us define :

$$Reach_T(A) = \{\omega \in \Omega \mid \exists t \in [0, T] : x_t(\omega) \in A\} \quad (2)$$

$$Reach_\infty(A) = \{\omega \in \Omega \mid \exists t \geq 0 : x_t(\omega) \in A\}. \quad (3)$$

These two sets are the sets of trajectories of M, which reach the set A (the flow that enters A) in the interval of time $[0, T]$ or $[0, \infty)$. The reachability problem consists of determining the probabilities of such sets. Since the process M is Borel right process and has the cadlag property, the reachability problem is well-defined, i.e. $Reach_T(A)$, $Reach_\infty(A)$ are indeed measurable sets - see Bujorianu et al. [2003]. Then the probabilities of reach events are

$$P(T_A < T) \text{ or } P(T_A < \zeta)$$

where ζ is the life time of M and T_A is the first hitting time of A :

$$T_A = \inf\{t > 0 | x_t \in A\}$$

and P is a probability on the measurable space $(\Omega, \mathcal{F})$ of the elementary events associated to M. P can be chosen to be P_x (if we want to consider the trajectories that start in x) or P_μ (if we want to consider the trajectories that start in with an initial condition given by the distribution μ). Recall that

$$P_\mu(A) = \int P_x(A) d\mu, A \in \mathcal{F}.$$

Remark 1. The probability $P(T_A < T)$, which is the probability of (2) can be thought of as a time-constrained reachability probability.

Denote by P_A the *hitting operator* associated to the underlying Markov process (x_t), i.e.

$$P_A v = E_x\{v \circ x_{T_A} | T_A < \zeta\}$$

and T_A is given by (3.1).

The following fundamental result of stochastic model checking was proved in Bujorianu et al. [2007].

Proposition 2. For any $x \in X$ and Borel set $A \in \mathcal{B}(X)$, we have

$$\varphi_A(x) = P_x[Reach_\infty(A)] = P_A 1(x).$$

In the next subsection, we will introduce the state constrained reachability probability.

3.2 State-Constrained Reachability

State-constrained reachability analysis denotes a reachability problem with additional conditions (constraints) on the system trajectories. Let us consider A, B two measurable sets of the state space X with disjoint closures, i.e. $A, B \in \mathcal{B}(X)$ and $\overline{A} \cap \overline{B} = \emptyset$. We consider two fundamental situations. Suppose that the system paths start from a given initial state x and we are interested in a target state set, let say B. These trajectories can hit a state set A or not. Therefore, we may define two new concepts:

- Obstacle avoidance reachability. In this interpretation B is a safe set, whilst A is not. The goal is to compute the probability $p_B^{A^c}(x)$ of all trajectories that start from a given initial state x and hit the set B without hitting the state set A (as illustrated in Fig.1).
- Waypoint reachability. In this interpretation we are intrested to compute the probability $p_B^A(x)$ of all trajectories that hit B only after hitting A (as illustrated in Fig.2).

The connection between the two types of stochastic reachability is given by the formula

$$p_B^{A^c}(x) + p_B^A(x) = \varphi_B(x)$$

where φ_B is the reachability function for the target set B given by formula (2). Therefore, the computability of the two types of reachability is equivalent. For technical reasons, it is more convenient to work with the waypoint reachability, which will be called from now on just simply *state-constrained reachability.*

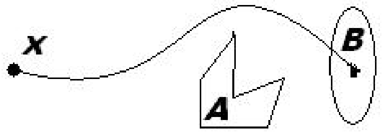

Fig. 1. Obstacle avoidance reachability

Now we consider the executions (paths) of the stochastic hybrid process that start in $x = (q, z) \in X$. When we investigate the state-constrained reachability, we ask the probability that these trajectories visit A before visiting eventually B. Mathematically, this is the probability of

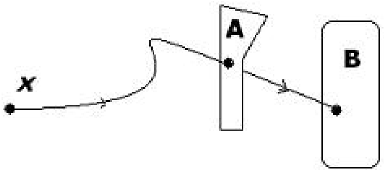

Fig. 2. Waypoint reachability

$$\{\omega | x_t(\omega) \notin B, t \leq T_A\}.$$

Moreover, using the first hitting time T_B of B, we are interested to compute

$$p(x) = P_x[T_A < T_B]$$

4. A QUALITATIVE STUDY OF STOCHASTIC MODEL CHECKING

It is known that the theory of Markov processes is intimately connected with the mathematical physics - see Blumenthal et al. [1968]. In potential theory, the physical interpretation of the state-constrained reachability probability considered in this paper is related to the *condenser problem* - see Blieder et al. [2004] and Chung et al. [1977]. This is described as follows: suppose we are given two disjoint compact conductors A, B in the Euclidean space $\mathbb{R}^3$ of positive capacity Ohtsuka [1975]. A positive electric unit charge placed on A and a negative unit charge on B, both allowed to distribute freely on the respective sets, will find a state of equilibrium, which is characterized on the one hand by minimal energy, and on the other hand by constant potential on A and on B (possibly taking out exceptional sets of zero capacity).

Then we have the following characterization.

Proposition 3. The state-constrained reachability probability p has the following properties:

(i) $0 \leq p \leq 1$ a.e. on X,

(ii) $p = 0$ a.e. on B, and $p = 1$ on A,

(iii) p is the potential of a signed measure ν such that the support of ν^+ is contained in A and the support of ν^- is contained in B.

We can write, in a more compact manner

$$p(x) = \begin{cases} P_x[T_A < T_B] & \text{if } x \notin A \cup B \\ 1 & \text{if } x \in A \\ 0 & \text{if } x \in B \end{cases}$$

An inclusion-exclusion argument leads to the following formula

$$\begin{aligned} p(x) &= P_x(T_A < T_B) \\ &= P_A 1(x) - P_B P_A 1(x) + P_A P_B P_A 1(x) - ... \end{aligned}$$

Proposition 4. Let $p_n = (P_A P_B)^n \varphi_A$, where φ_A is given by (2). Then

$$p = \sum_{n=0}^{\infty} (p_n - P_B p_n).$$

Proof. Each p_n is an excessive function, bounded by 1, and $P_B p_n \leq p_n$. Therefore,

$$p_n - P_B p_n \in [0,1].$$

Let us set $T_0 := 0$ and $T_1, T_2, T_3, ...$ are the times of the successive visits to A, then to B, then back to A, and so on. Formally, these times are defined as:

$$\begin{aligned} T_1 &:= T_A \\ T_2 &:= T_A + T_B \circ \theta_{T_A} \\ &... \\ T_{2n+1} &:= T_{2n} + T_A \circ \theta_{T_{2n}} \\ T_{2n+2} &:= T_{2n+1} + T_B \circ \theta_{T_{2n+1}} \end{aligned}$$

An induction argument shows that

$$P_{T_{2n}} = (P_A P_B)^n,\ n \in \mathbb{N}.$$

Then, it can be easily checked that

$$P_x[T_A < T_B, T_{2n+1} \leq L \leq T_{2n+2}] = p_n(x) - P_B p_n(x)$$

where L is the last exit time from A, i.e.

$$L = L_A = \sup\{t > 0 | x_t \in A\}.$$

L is a.e. finite because usually we suppose that our process is transient, in the sense that if it enters a set then it must leave it also. ■

Theorem 5. State-constrained reachability probability p solves the following boundary value problem:

$$\begin{array}{ll} \mathcal{L}p(x) = 0 & x \in X \backslash (A \cup B) \\ p(x) = 1 & x \in A \\ p(x) = 0 & x \in B. \end{array}$$

where $\mathcal{L}$ is the infinitesimal generator of the stochastic hybrid process given by (1).

This is the main theorem about the characterization of the state-constrained reachability. The theorem can be proved for Borel right processes that are SH processes. Stochastic hybrid processes have a continuous dynamics given by some diffusion processes, and a discrete dynamics described by a Markov chain. Therefore, the proof is a consequence of the following two lemmas, which are instantiations of the theorem for Brownian motion and Markov chains. We have not found the proofs in any monograph of stochastic processes - for example Grimmett et al. [1982], therefore we sketch these proofs in the following.

Lemma 6. Let us consider a (discrete time, discrete state) Markov chain (X_t) with the state space Γ and the one-step transition function $p_1(x,y)$ Given two disjoint sets $A, B \subset \Gamma$. Then the state-constrained reachability probability $p(x)$ is the solution of the boundary value problem

$$\begin{array}{ll} (1-p_1)p(x) = 0 & x \in \Gamma \backslash (A \cup B) \\ p(x) = 1 & x \in A \\ p(x) = 0 & x \in B. \end{array}$$

Remark 2. For a discrete discrete space Markov chain, it is known that its infinitesimal generator is given by

$$\mathcal{L} = 1 - p_1$$

Proof. If $x \notin A \cup B$, we make the elementary remark that the first step away leads either to B, and the event $\{T_A < T_B\}$ fails to happen, or to A, in which case the event happens, or to another point $y \notin A \cup B$, in which case the event happens with probability $P_y[T_A < T_B]$. Therefore, we obtain

$$P_x[T_A < T_B] = \sum_{y \in A} p_1(x,y) + \sum_{y \notin A \cup B} P_y[T_A < T_B].$$

Then for $x \notin A \cup B$, we obtain

$$p(x) = \sum_{y \in \Gamma} p_1(x,y) p(y).$$

That ends the proof. ■

Lemma 7. Let us consider W the standard d-dimensional Wiener process. Let A, B be two disjoint capacitable sets (see Sion [1963] for full definition) of non-zero capacity such that $A \cup B$ is closed. The reachability probability $p(x)$ satisfies the Laplace problem

$$\nabla^2 p(x) = 0$$

on $X - (A \cup B)$ with the boundary condition

$$p(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \in B \end{cases}$$

Proof. . Let $x \in X - (A \cup B)$ and H a ball of radius h and surface S in $X - (A \cup B)$ centred in x. Define the random variable $T = \inf\{t | x_t(\omega) \in S\}$. This has the property that $P_x[T < \infty] = 1$. Let $H_i = \{|W(i) - W(i-1)| \leq 2h\}$. Then $P_x(A_1) < 1$ and $\lim_{n \to \infty} P_x[T > n] = 0$. This results from the inequality $P_x[T > n] \leq P_x(A_1 \cap ... \cap A_n) = P_x(A_1)^n$.

We have

$$p(x) = \int_{y \in S} P_x[T_A < T_B | W(T) = y] f(y) dS.$$

where $f(y) = 1/|S|$ is the density function. This means that

$$p(x) = \int_{y \in S} p(y)/|S| dS. \blacksquare$$

5. CONCLUSIONS

In this paper, the stochastic reachability problem for stochastic hybrid systems has been specialized by introducing constraints relative to the state space. We have proved that the state-constrained stochastic reachability is solvable

The natural next step will be to derive numerical approximation algorithms and to study their complexity. In a future work, we intend to apply our approach to problems in the areas of control engineering and path planning.

An immediate problem in control engineering can be defined as follows. Suppose that the probability of reaching a target set by avoiding a dangerous state set, for a given control strategy, is quite small. That means a new control strategy needs to be defined in order to maximize this probability, i.e. smarter method has to be found to avoid danger by obtaining the objective.

An application at hand is for *autonomous aerial vehicles* (UAVs) in a combat situation. The interpretation of the state-constrained reachability is quite obvious. Once a hostile area (perhaps an artillery unit) is discovered, the flying robot has to estimate if the current planned trajectory and its possible perturbations will visit the target area by avoiding the hostile one. When this estimation is pessimistic (with small probability), then an avoidance strategy should be applied.

This work is part of a more general programme called *Hilbertean Formal Methods* (we refer the reader to the manifesto paper Bujorianu [2007] and the most recent development Bujorianu [2009]). The Hilbertean formal methods combine the formal approach from software engineering with methods from continuous mathematics to investigate qualitative properties of hybrid, embedded or control systems. It models uniformly the deterministic and the stochastic systems, and the verification methods rely on the stochastic model checking, as developed in this paper. There are good reasons for scaling the model checking of stochastic hybrid systems to complex systems like the *cyber-physical systems*. The cyber-physical systems are defined as networks of functional units that involve a tight interaction of physics and computation. The interaction can take the form of control, activity coordination, resource management, and so on.
The connection between hybrid system reachability and mathematical physics gets an ad litteram interpretation in nano-technology. The future nano-systems (we refer the reader to the comprehensive monograph Hornyak et al. [2008]) will be self-assembled (and thus subjects to many defects), deployed in very harsh environments and their behavior will be random and error prone. The nano-robots deployed in critical situations (like drugs carriers or viruses killers) will need to be safety verified, and most of the classical verification methods are not applicable in a context of a high uncertainty and fault tolerance.

ACKNOWLEDGEMENTS

This research was funded by the EPSRC project EP/ E050441/1: The Manchester Centre for Interdisciplinary Computational and Dynamical Analysis (CICADA).

REFERENCES

C. Baier, B.J. Haverkort, H. Hermanns, J.P. Katoen. Reachability in Continuous-Time Markov Reward Decision Processes. *Logic and Automata: History and Perspectives*, pages 53–71, 2007.

J. Bliedtner, M. Musat. The condenser problem. *Potential Anal.*, 21, No.2, pages 177–192, 2004.

H.A.P. Blom, J. Lygeros, editors. *Stochastic Hybrid Systems: Theory and Safety Critical Applications.* LNCIS 337, 2006.

H.A.P. Blom, G.J. Bakker, J. Krystul. Probabilistic reachability analysis for large scale stochastic hybrid systems. 46th IEEE Conference on Decision and Control, pages 3182–3189, 2007.

R.M. Blumenthal, R.K. Getoor. *Markov Processes and Potential Theory.* Academic Press, New York and London 1968.

M.L. Bujorianu, J. Lygeros, R. Langerak. Reachability Analysis of Stochastic Hybrid Systems by Optimal Control. HSCC, LNCS 4981, pages 610–613, 2008.

M.L. Bujorianu, M.C. Bujorianu. Co-Evolution Preserving Abstract Model Reduction For Uncertain Cyber-Physical Systems. *Proc. of the 6th International Conference on Informatics in Control, Automation and Robotics - ICINCO.* INSTIC Press, 2009.

M.C. Bujorianu, M.L. Bujorianu. Towards Hilbertian Formal Methods. *Proc. of the 7th International Conference on Application of Concurrency to System Design - ACSD.* IEEE Press, 2007.

M.L. Bujorianu, J. Lygeros. Towards Modelling of General Stochastic Hybrid Systems In Blom et al. [2006], pages 3–30.

M.L. Bujorianu. A Statistical Inference Method for the Stochastic Reachability Analysis. CDC-ECC'05. 44th IEEE Conference on Decision and Control, pages 8088–8093, 2005.

M.L. Bujorianu, J. Lygeros. New Insights on Stochastic Reachability. 46th Conference in Decision and Control, pages 6172–6177, 2007.

M.L. Bujorianu, J. Lygeros. General Stochastic Hybrid Systems: Modelling and Optimal Control. 43th Conference in Decision and Control, pages 1872–1877, Vol.2, 2004.

M.L. Bujorianu, J. Lygeros. Reachability Questions in Piecewise Deterministic Markov Processes HSCC, LNCS 2623, pages 126–140, 2003.

K.L. Chung, R.K. Getoor. The Condenser Problem. *The Annals of Probability*, **5** (1), pages 82–86, 1977.

M.H.A. Davis. *Markov Models and Optimization.* Chapman and Hall, 1993.

S.N. Ethier, T.G. Kurtz. *Markov Processes: Characterization and Convergence.* New York: John Wiley and Sons, 1986.

G. Grimmett, D. Stirzaker. *Probability and Random Processes.* Oxford University Press, 1982.

G. Hornyak, J. Dutta et. al. *Introduction to Nanoscience.* CRC Press, 2008.

J. Krystul, H.A.P. Blom. Sequential Monte Carlo Simulation of Rare Event Probability in Stochastic Hybrid Systems. 16th IFAC World Congress, 2005.

X. Koutsoukos, D. Riley. Computational Methods for Verification of Stochastic Hybrid Systems. *IEEE Trans. on Systems, Man and Cybernetics.* Part A., Volume 38, Issue 2, Pages 385–396, March 2008.

M. Ohtsuka. A general definition of capacity. *Annales de l'Institut Fourier*, 25 no. 3-4, pages 499–507, 1975.

M. Prandini, J. Hu. A Stochastic Approximation Method for Reachability Computations. In Blom et al. [2006], pages 107–139.

M. Sion. On capacitability and measurability. *Annales de l'Institut Fourier*, 13 no. 1, pages 83–98, 1963.