Proceedings of the
44th IEEE Conference on Decision and Control, and
the European Control Conference 2005
Seville, Spain, December 12-15, 2005

Abstractions of Stochastic Hybrid Systems

Manuela L. Bujorianu, Marius C. Bujorianu, and John Lygeros

Abstract— **Many control systems have large, infinite state space that can not be easily abstracted. One method to analyse and verify these systems is reachability analysis. It is frequently used for air traffic control and power plants. Because of lack of complete information about the environment or unpredicted changes, the stochastic approach is a viable alternative. In this paper, different ways of introducing rechability under uncertainty are presented. A new concept of stochastic bisimulation is introduced and its connection with the reachability analysis is established. The work is mainly motivated by safety critical situations in air traffic control (like collision detection and avoidance) and formal tools are based on stochastic analysis.**

Keywords: stochastic hybrid systems, bisimulation, reachability analysis, Markov processes.

I. Introduction

Safety-critical embedded systems like those arising from air traffic control have, in general, infinite continuous state space. Verification of safety properties is crucial, but very difficult or almost impossible for these systems. In this paper we propose a probabilistic approach such that safety properties can be checked with some degree of 'accuracy'. When the probability of a critical situation is very small, this situation could happen in extremely rare cases. When the previous probability has a significant value (let say over a prescribed threshold) then the system behaviour could be considered dangerous. One can get more confidence in the system reliability when probabilities are calculated to be small enough. This approach is getting more important especially when formal verification is not available or is not made available in reasonable time.

There is no uniform way stochastic aspects are considered in control engineering. In this paper, we distinguish between probabilistic approaches and stochastic approaches. In the probabilistic approach, probabilities are introduced as discrete distributions of

- the possible initial system states;
- the possible transitions from an arbitrary state [21].

These precise functions of probabilities (basically, to realize quantification of non-determinism) make verification tractable: Markov chain models can be constructed and model checking is possible.

In the stochastic approach, probabilities measure only

- sets of all paths between two arbitrary states, or
- sets of paths, all starting from the same state and ending in a specified set of states (stochastic kernels).

M.L. Bujorianu is with Faculty of Computer Science, University of Twente, 7500 AE Enschede, The Netherlands, mlb@cs.stir.ac.uk

M.C. Bujorianu is with Computing Laboratory, University of Kent, Canterbury, CT2 7NF, UK mcb8@kent.ac.uk

J. Lygeros is with Department of Electrical and Computer Engineering, University of Patras, Patras, GR26500, Greece lygeros@ee.upatras.gr

Formal verification in the stochastic case is hard (very often Markov chains are not available), usually engineering methods like Monte Carlo simulation [15] being used. But the increased amount of stochastic models in distributed systems applications, like computer networks and air traffic control, put pressure on finding more verification techniques.

In this paper we define a new stochastic bisimulation concept for a class of Markov processes based on the notions of capacity and measurable relation. A measurable relation between two processes is a relation on the product of their state spaces, which induces two hoemeomorphic quotient measurable spaces. A capacity is non-additive set-function used to represent uncertainty. The mathematical theory of non-additive set-functions got its first contribution with Gustave Choquet's "Theory of Capacities" [6] in 1953. Choquet's interest was applications to statistical mechanics and potential theory. Later this theory found applications in decision theory [8], [23], robust Bayesian inference [14], artificial intelligence and automated reasoning [9], finance and asset pricing [10], etc.

Each process can have associated, in a canonical way, a Choquet capacity (see subsection II-C). A bisimulation relation between two processes is defined as a measurable relation that "preserves" the capacity. Further, we have employed this bisimulation to define bisimulation between stochastic hybrid systems whose realizations (all possible executions) are Markov processes as above. Moreover, we figure out connections between stochastic bisimulation and stochastic reachability. This approach on bisimulation is complementary to the one presented in [5] based on category theory.

Moreover, using the concept integrale with respect to a capacity (see subsection II.A) we introduce a pseudometric between processes. The distance between two processes is measured in terms of probabilities of the set of trajectories which ever visit the sets that can be "identified" through the homeomorphism induced by a measurable relation.

The basic ingredients we use are Markov processes and the associated semigroups and capacities.

The paper is structured as follows. In the next section we present a short background on capacities and Markov processes. After, these notions will be employed to define a new concept of stochastic bisimulation (section III). Then, in section IV we make the connection between this bisimulation and stochastic reachability. The paper ends with a quick overview of related work and a final remark on the dependability of our approach.

II. Background

0-7803-9568-9/05/$20.00 ©2005 IEEE

In this section we present some results about Markov processes and capacities.

A. Stochastic analysis of Markov processes

We fix $(\Omega, \mathcal{F})$ a measurable space. Let $\mathcal{M}_t$, $t \in [0,\infty]$ be sub-σ-algebras of $\mathcal{F}$. $(\mathcal{M}_t) := (\mathcal{M}_t)_{t\in[0,\infty]}$ is called a filtration on $(\Omega, \mathcal{F})$ if $\mathcal{M}_t$ is increasing in t and $\mathcal{M}_\infty = \bigvee_{t\in[0,\infty)} \mathcal{M}_t$, i.e. $\mathcal{M}_\infty$ is the smallest σ-algebra containing all $\mathcal{M}_t$, $t \in [0,\infty)$. A filtration $\{\mathcal{M}_t\}$ is *right continuous* if $\mathcal{M}_t = \mathcal{M}_{t+} = \cap\{\mathcal{M}_{t'} | t' > t\}$. Let X be a topological Hausdorff space and assume that $\mathcal{B}$ is the Borel σ-algebra of X. We adjoin an extra point Δ (the cemetery) to X as an isolated point, $X_\Delta = X \cup \{\Delta\}$. Let $\mathcal{B}(X_\Delta)$ be the Borel σ-algebra of X_Δ.

Let $\mathbb{M} = (\Omega, \mathcal{F}, (x_t)_{t\geq 0}, (P_x)_{x\in X_\Delta})$ be a Markov process with the state space $(X, \mathcal{B})$, life time $\zeta(\omega)$ (when the process $\mathbb{M}$ escapes to and is trapped at Δ) and corresponding filtration $(\mathcal{M}_t)$. The elements $\mathcal{F}_t^0$, $\mathcal{F}_t$, P_x are defined as follows.

• $\mathcal{F}_t^0$ is the *natural filtration*, i.e. $\mathcal{F}_t^0 = \sigma\{x_t, s \leq t\}$ for $t \in [0,\infty]$. Then $\mathcal{F}_t^0$ is the *minimum admissible filtration* (i.e., $\forall t \in [0,\infty]$, $(x_t)_{t\geq 0}$ is adapted w.r.t. $(\mathcal{F}_t^0)$).

• $P_x : (\Omega, \mathcal{F}) \to [0,1]$ is a probability measure (called *Wiener probability*) such that $P_x(x_t \in E)$ is $\mathcal{B}$-measurable in $x \in X$ for each $t \geq 0$ and $E \in \mathcal{B}$.

• If $\mu \in \mathcal{P}(X_\Delta)$, i.e. μ is a probability measure on $(X_\Delta, \mathcal{B}(X_\Delta))$ then we can define

$$P_\mu(\Lambda) = \int_{X_\Delta} P_x(\Lambda)\mu(dx), \Lambda \in \mathcal{F}.$$

The completion of $\mathcal{F}_t^0$, for $t \in [0,\infty]$, w.r.t. all P_μ, $\mu \in \mathcal{P}(X_\Delta)$, is denoted by $\mathcal{F}_t$.

Given an admissible filtration $\{\mathcal{M}_t\}$, a $[0,\infty]$-valued function τ on Ω is called an $\{\mathcal{M}_t\}$-*stopping time* if $\{\tau \leq t\} \in \mathcal{M}_t$, $\forall t \geq 0$.

For an admissible filtration $\{\mathcal{M}_t\}$, we say that $\mathbb{M}$ is *strong Markov* w.r.t. $\{\mathcal{M}_t\}$ if $\{\mathcal{M}_t\}$ is right continuous and for any $\{\mathcal{M}_t\}$-stopping time τ

$$P_\mu(x_{\tau+t} \in E | \mathcal{M}_\tau) = P_{x_\tau}(x_t \in E);\ P_\mu - a.s.$$

$\mu \in \mathcal{P}(X_\Delta)$, $E \in \mathcal{B}$, $t \geq 0$.

$\mathbb{M}$ has the *càdlàg property* if for each $\omega \in \Omega$, the sample path $t \mapsto x_t(\omega)$ is right continuous on $[0,\infty)$ and has left limits on $(0,\infty)$ (inside X_Δ).

Let (P_t) denote the operator semigroup associated to $\mathbb{M}$ which maps $\mathcal{B}^b(X)$ (the set of all bounded measurable functions on X) into itself given by

$$P_t f(x) = E_x f(x_t),$$

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

B. Capacities

The information input into different real-world models may be imprecise for several reasons. For example, for computer models, imprecision is often a consequence of measurement processes (e.g. using digital sensors). Prior information is sometime recorded in the literature as intervals without any information about probability distributions [8].

The extension of probabilistic analysis to include imprecise information is now well established in the theory of imprecise probabilities [28], robust Bayesian analysis [16] and fuzzy statistics [27].

The imprecise probabilities are modelled by sets of probability measures which might generate upper/lower probabilities [8], [11], Choquet capacities [6], [14], etc.

In the following, first, we shortly present the concept of Choquet capacity and then we give the construction of the capacity associated to a Borel right Markov process. This later concept is used in the next section to give a new definition for stochastic bisimulation.

Intuitively, a capacity is a set function which extend the concept of measure. The additivity property is not longer true for a capacity.

For every space X and algebra $\mathcal{A}$ of subsets of X a set-function $c : \mathcal{A} \to [0,1]$ is called a *normalized capacity* if it satisfies the following:

(i) $c(\emptyset) = 0$, $c(X) = 1$,

(ii) $\forall A, B \in \mathcal{A}$: $A \subset B \Rightarrow c(A) \leq c(B)$.

A capacity is called *convex (or supermodular)* if in addition to (i)-(ii) it satisfies the additional property

(iii) $\forall A, B \in \mathcal{A}$: $c(A \cup B) \geq c(A) + c(B) - c(A \cap B)$.

A special type of convex capacities are the *belief functions* presented and discussed by Dempster [8] and Shafer [22]. A capacity is called a probability if (iii) holds everywhere with equality, i.e. it is additive. If a capacity satisfies the inverse inequality in (iii) then it is called *submodular or strongly subadditive*.

Since we allow the possibility that c is not additive, we can not use the integral in the Lebesgue sense to integrate w.r.t. c. The notion of integral we use is due originally to Choquet [6] and it was independently rediscovered and extended by Schmeidler [23]. If $f : X \to \mathbb{R}$ is bounded $\mathcal{A}$-measurable function and c is any capacity on X we define the Choquet integral of f w.r.t. c to be the number

$$\begin{aligned}\int_X f(x)dc(x) &= \int_0^\infty c(\{x \in X | f(x) \geq \alpha\})d\alpha + \\ &+ \int_{-\infty}^0 [c(\{x \in X | f(x) \geq \alpha\}) - 1]d\alpha\end{aligned}$$

where the integrals are taken in the sense of Riemann.

C. Markov Process Capacity

Throughout this paper $M = (\Omega, \mathcal{F}, \mathcal{F}_t, x_t, P_x)$ will be a Borel right Markov process on $(X, \mathcal{B})$. This means that (see, for example, [7] and the references therein):

• Its state space $(X, \mathcal{B})$ is a Lusin state space (i.e. X is a separable metric space homeomorphic to a Borel subset of some compact metric space, with Borel σ-algebra $\mathcal{B}(X)$ or shortly $\mathcal{B}$). It will be equipped with a σ-finite measure m.

• M is a strong Markov process and the sample paths $t \to x_t(\omega)$ are almost surely right continuous.

• the transition operator semigroup $(P_t)_{t\geq 0}$ of M maps $\mathcal{B}^b$ (the lattice of bounded real measurable functions defined on X) into itself.

In addition, in this paper we suppose that M has the cadlag property. We assume also that M is *transient*. This means that there exists a strictly positive Borel function q such that Uq is bounded (where $Uf = \int_0^\infty P_t f dt$ is the *kernel operator*). More, we suppose that $\sup_{x\in X} U1(x) < \infty$. For each $x \in X$, the kernel U will provide a measure U_x defined by $U_x(A) = UI_A(x), \forall A \in \mathcal{B}$ and for any measurable positive function f on X we have $Uf(x) = \int f dU_x$. More, we have

$$U_x(A) = (m \otimes P_x)(\{(t,\omega)|x_t(\omega) \in A\}).$$

Therefore, $U_x(A)$ 'measures' two aspect: (i) the length of time spent by the process in A and (ii) the probability of the trajectories which start in x and reach A at some times $t \in [0,\infty)$.

One can take the sample space Ω for M to be the set of all paths $(0,\infty) \ni t \mapsto \omega(t) \in X_\Delta$ such that (i) $t \mapsto \omega(t)$ is X-valued and cadlag on $(0, \zeta(\omega))$ where $\zeta(\omega) := \inf\{s > 0|\omega(s) = \Delta\}$, (ii) $\omega(t) = \Delta$ for all $t \geq \zeta(\omega)$, and (iii) $\zeta(\omega) < \infty$. In this way, M is realized as the coordinate process on Ω: $x_t(\omega) = \omega(t)$, $t > 0$. We complete the definition of M by declaring $x_0(\omega) = \lim_{t\searrow 0} \omega(t)$, $t > 0$.

Because of transience condition, the measure m is purely excessive [13]:

$$\lim_{t\to\infty}(m < P_t >)(A) = 0, \forall A \in \mathcal{B} \text{ with } m(A) < \infty,$$

where $(m < P_t >)(A) = \int p_t(x,A)m(dx)$ and $p_t(x,A) = P_t(I_A)(x) = P_x(x_t \in A)$.

Consequently there is a unique entrance law $(\mu_t)_{t>0}$ (a family of σ-finite measures on $(X,\mathcal{B})$ with $\mu_t < P_s >= \mu_{t+s}$ for all $t,s > 0$) such that $m(A) = \int_0^\infty \mu_t(A)dt$, $\forall A \in \mathcal{B}$. See, for example, [13] for more details. Then there is a σ-finite measure $\mathbb{P}$ on $(\Omega, \mathcal{F}_t^0)$ (see [12]) under which the coordinate process $(x_t)_{t>0}$ is Markovian with transition semigroup $(P_t)_{t\geq 0}$ and one-dimensional distributions $\mathbb{P}(x_t \in A) = \mu_t(A)$, $\forall A \in \mathcal{B}$, $t > 0$.

The *capacity* associated to M is defined as follows (see [12] and the references therein): for all $B \in \mathcal{B}$

$$Cap_M(B) = \mathbb{P}(T_B < \infty) = \mathbb{P}(T_B < \zeta), \qquad (1)$$

where T_B is the first hitting time of B, i.e. $T_B = \inf\{t > 0|x_t \in B\}$.

This capacity can be written as a non-additive set function $Cap_M : (X,\mathcal{B}) \to [0,1]$, which is finer than a measure. The capacity of a measurable set B can be thought of as a 'measure' of all process trajectories that ever visit B over an infinite horizon time. It can be shown that Cap_M is monotone increasing, submodular, and countably subadditive [12]. The initial definition (see the references therein [12]) of this notion gives the capacity Cap_M as an upper envelope of a non-empty class of probability measures on $\mathcal{B}$. Then its conjugate Cap_M^* [23], defined by $Cap_M^*(B) = 1 - Cap_M(X - B)$ is a belief function in sense of [22].

III. Bisimulation

Let $(X,\mathcal{B}(X))$ and $(Y,\mathcal{B}(Y))$ be Lusin spaces[1] and let $\mathcal{R} \subset X \times Y$ be a relation such that $\Pi^1(\mathcal{R}) = X$ and $\Pi^2(\mathcal{R}) = Y$. We define the equivalence relation on X that is induced by the relation $\mathcal{R} \subset X \times Y$, as the transitive closure of $\{(x,x')|\exists y \text{ s.t. } (x,y) \in \mathcal{R} \text{ and } (x',y) \in \mathcal{R}\}$. Analogously, the induced (by $\mathcal{R}$) equivalence relation on Y is defined. We write $X/_\mathcal{R}$ and $Y/_\mathcal{R}$ for the sets of equivalence classes of X and Y induced by $\mathcal{R}$. We denote the equivalence class of $x \in X$ by $[x]$. We define now the notion of *measurable relation*. Let $\mathcal{B}^*(X) = \mathcal{B}(X) \cap \{A \subset X|$ if $x \in A$ and $[x] = [x']$ then $x' \in A\}$ be the collection of all Borel sets in which any equivalence class of X is either totally contained or totally not contained. It can be checked that $\mathcal{B}^*(X)$ is a σ-algebra. Let $\pi_X : X \to X/_\mathcal{R}$ be the mapping that maps each $x \in X$ to its equivalence class and let

$$\mathcal{B}(X/_\mathcal{R}) = \{A \subset X/_\mathcal{R}|\pi_X^{-1}(A) \in \mathcal{B}^*(X)\}.$$

Then $(X/_\mathcal{R}, \mathcal{B}(X/_\mathcal{R}))$, which is a measurable space, is called the quotient space of X w.r.t. $\mathcal{R}$. The quotient space of Y w.r.t. $\mathcal{R}$ is defined in a similar way. We define a bijective mapping $\psi : X/_\mathcal{R} \to Y/_\mathcal{R}$ as $\psi([x]) = [y]$ if $(x,y) \in \mathcal{R}$ for some $x \in [x]$ and some $y \in [y]$. We say that the relation $\mathcal{R}$ is *measurable* if X and Y if for all $A \in \mathcal{B}(X/_\mathcal{R})$ we have $\psi(A) \in \mathcal{B}(Y/_\mathcal{R})$ and vice versa, i.e. ψ is a homeomorphism. Then the real measurable functions defined on $X/_\mathcal{R}$ can be identified with those defined on $Y/_\mathcal{R}$ through the homeomorphism ψ. We can write $\mathcal{B}^b(X/_\mathcal{R}) \overset{\psi}{\cong} \mathcal{B}^b(Y/_\mathcal{R})$. Moreover, these functions can be thought of as real functions defined on X or Y measurable w.r.t. $\mathcal{B}^*(X)$ or $\mathcal{B}^*(Y)$.

In the following we introduce a new concept of equivalence between two capacities with respect to a measurable relation defined on the product of their underlying spaces.

Definition 1: Suppose we have the capacities c_X and c_Y on the Lusin spaces $(X,\mathcal{B}(X))$ and $(Y,\mathcal{B}(Y))$ respectively and a measurable relation $\mathcal{R} \subset X \times Y$. The capacities c_X and c_Y are called equivalent w.r.t. $\mathcal{R}$ if they define the same capacity on the quotient space of X and Y, i.e. if we have $c_X(\pi_X^{-1}(A)) = c_Y(\pi_Y^{-1}[\psi(A)])$ for all $A \in \mathcal{B}(X/_\mathcal{R})$.

Suppose we have two Borel right Markov processes M and W with the state spaces X and Y. The equivalence between capacities will be employed in defining a new 'equivalence' between Markov processes, as follows.

Definition 2: A measurable relation $\mathcal{R} \subset X \times Y$ is a bisimulation between M and W if their associated capacities Cap_M and Cap_W are equivalent w.r.t. $\mathcal{R}$.

It is known that for symmetric processes (equal with their time reversed processes) defined on the same state space, the equality of their capacities implies that they are time changes of one another [12].

We can define now a *pseudometric with respect a measurable relation* $\mathcal{R} \subset X \times Y$ between the processes M and

[1]The equivalence relation introduced in this section can be defi ned in a more general setting of the analytic spaces.

W as follows:

$$d_{\mathcal{R}}(M,W) = \sup_{f\in\mathcal{B}^{*b}(X)} |\int f dCap_M - \int f\circ\psi dCap_W|$$

where $\mathcal{B}^{*b}(X)$ is the set of bounded real $\mathcal{B}^*(X)$-measurable functions on X.

Remark 1: We can define a distance between two processes if and only there exists a measurable relation on the product of their state spaces $X \times Y$. Or, equivalently, if and only if there exists a third measurable space $(Z, \mathcal{B}(Z))$ and two surjective measurable mappings $\phi_1 : X \to Z$ and $\phi_2 : Y \to Z$ then

$$d(M,W) = \sup_{f\in\mathcal{B}^{b}(Z)} |\int f\circ\phi_1 dCap_M - \int f\circ\phi_2 dCap_W|$$

where $\mathcal{B}^b(Z)$ is the set of bounded real $\mathcal{B}^b(Z)$-measurable functions on Z.

Proposition 1: A measurable relation $\mathcal{R} \subset X \times Y$ is a bisimulation between M and W if and only if

$$d_{\mathcal{R}}(M,W) = 0$$

In the classical theory of stochastic processes, one process is a modification of another iff their transition probabilities differ on set of times of measure zero.

Proposition 2: A Borel right Markov process is bisimilar with any of its modifications.

We can refine further this result by considering another way to define equivalence between stochastic processes. Two Markov processes are equivalent if they possess a common exceptional set (a set with zero capacity) outside which their transition functions coincide.

Proposition 3: Two equivalent Markov processes are bisimilar.

The way to define bisimulation between two Markov processes is, in fact, a new approach to define coarser versions of the concept of equivalence between stochastic processes. In this approach, two processes are bisimilar (weak equivalent) if one can define an equivalence relation on the product of their state spaces such that the quotient processes have associated equal capacities (i.e. this weak equivalence preserves the probability to 'reach' certain state spaces over infinite horizon time).

EXAMPLE

We consider now a simplified situation in air traffic control. A stochastic model of commercial flights from London's airports Stansted and Gatwick to Paris is constructed. This model varies periodically, as there are constant changes in weather influence (strong winds, storms, dark clouds, etc) and local traffic (for example, domestic flights from Ashford Airport or traffic between Europe and the States). This influences are captured in the definition of various concepts that characterise a Markov process. Often, in such models the set of trajectories starting from Stansted and passing through Kent county (the area marked II on the map from Fig. 1) has the same probability with the set of trajectories starting from Gatwick and passing through Sussex county (the area marked I on the map from Fig. 1). This is because the weather in the two counties is very similar and the local traffic presents the same characteristics.

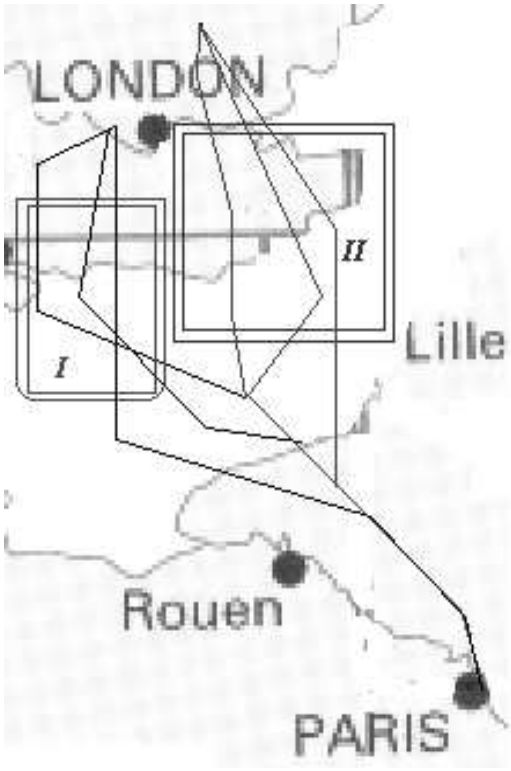

Fig. 1.

The Markov process illustrated in Fig. 1 is bisimilar with the one illustrated in Fig. 2. The bisimilarity should not be considered as a refinement game of partitions of a geographical area. The Air Traffic Control system state space is actually given by the Borel sets of the Euclidean space. This is because, in the air traffic controller representation of a plane position, not the actual, precise (like latitude and longitude) position is consider, but a larger area, that can be measured by a probability. In other words, it does not really matter if the plane is actually 30 meters away from the controller's representation. In this example, the two counties are bisimilar from the perspective of weather conditions and the local traffic on some routes.

IV. Stochastic Reachability and Bisimulation

One of the most important goals of our work [3], [4], [20] was to develop formal mathematical models for the *safety critical air traffic management situations.* A central problem in air traffic control is determining the conflict probability, i.e. the probability that two aircraft come closer than a minimum allowed distance. If this probability can be computed, an alert can be issued when it exceeds a certain threshold.

In the context of stochastic hybrid systems, the computation of the conflict probability reduces to a *reachability*

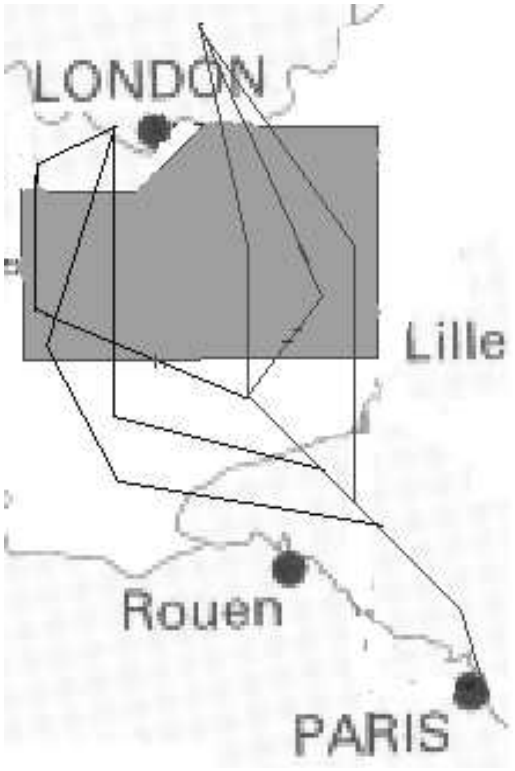

Fig. 2.

problem: *computing the probability that the stochastic hybrid process modelling the aircraft motion reaches an unsafe part of the state space* (where two aircraft come closer than the minimum allowed distance).

In a probabilistic framework, the reachability problem consists of determining the probability that the system trajectories enter some prespecified set starting from a certain set of initial conditions with a given probability distribution.

Stochastic hybrid systems are 'traditional' hybrid systems with some stochastic features. These systems typically contain variables or signals that take values from a continuous set and also variables that take values from a discrete (finite or countable) set. Differential equations or stochastic differential equations generally give the continuous dynamics of such systems. A Markov chain generally governs the discrete-variable dynamics of stochastic hybrid systems. The stochastic features might be present in the continuous dynamics or in the discrete dynamics, or in both. The continuous and discrete dynamics coexist and interact with each other and because of this it is important to use models that accurately describe the dynamic behaviour of such hybrid systems. The realizations of the different models of stochastic hybrid systems (see [20] for an overview) can be thought of as particular classes of strong Markov processes with the continuous evolution disturbed by forced or spontneous transitions.

Let us consider $M = (\Omega, \mathcal{F}, \mathcal{F}_t, x_t, P_x)$ a Borel right Markov process, as the realization of a stochastic hybrid system H. To address the reachability problem assume that we have a given set $E \in \mathcal{B}(X)$ and a horizon time $T > 0$. Let us to define:

$$\begin{aligned} Reach_T(E) &= \{\omega \in \Omega \mid \exists t \in [0,T] : x_t(\omega) \in E\} \\ Reach_\infty(E) &= \{\omega \in \Omega \mid \exists t \geq 0 : x_t(\omega) \in E\}. \end{aligned} \quad (2)$$

These two sets are the sets of trajectories of M, which reach the set E (the flow that enters E) in the interval of time $[0,T]$ or $[0,\infty)$. The reachability problem consists of determing the probability of such sets. That means we have to determine $\mathbb{P}(T_E < T\infty)$ or $\mathbb{P}(T_E < \infty)$. In this way, the reachability problem is related with the computation of the capacities associated to the processes M_T and M, where M_T is the process M "killed" after the time T (see [7] for the details about the killed process).
On the other hand, we want to characterise the sets

$$\begin{gathered} Reach_T^{init}(E) = \\ = \{x \in X | \exists \omega \in \Omega, \exists t \in [0,T] : \phi(t,\omega,x) \in E\} \\ Reach_\infty^{init}(E) = \\ = \{x \in X | \exists \omega \in \Omega, \exists t \in [0,\infty) : \phi(t,\omega,x) \in E\} \end{gathered}$$

where $\phi(t,\omega,x)$ is a trajectory of M starting with $x \in X$. These are sets of initial points, which give trajectories of M with nonempty intersection with E.

Lemma 4: For any $T > 0$ and $E \in \mathcal{B}$, we have

$$Reach_T^{init}(E) = \{x \in X | \sup_{t \in [0,T]} P_t I_E(x) > 0\}.$$

Proposition 5: If M has the càdlàg property and G is an open set of X then

$$Reach_\infty^{init}(G) = \{x \in X | U_x(G) > 0\}.$$

Remark 2: The measure U_x does not have enough ability for our purposes: a trajectory ω that reaches the set E is accounted for every 'visit' in E. This weakness is eliminated when considering the measure $\mathbb{P}(T_E < \infty)$.

Suppose we have given two stochastic hybrid systems H and H' with the realizations M and W (with the state spaces X and Y). Two stochastic hybrid systems are bisimilar iff their realizations are bisimilar. Formally, this bisimulation can be defined as follows.

Definition 3: H and H' are bisimular if there exists a measurable relation $\mathcal{R} \subset X \times Y$ such that $\mathcal{R}$ is a bisimulation between M and W.

Proposition 6: $\mathcal{R} \subset X \times Y$ is a bisimulation relation between H and H' with the realizations M and W (whose state spaces are X and Y) iff the probabilities of reachable events (2) associated to "saturated" (w.r.t. $\mathcal{R}$) Borel sets are equal, i.e.

$$\mathbb{P}_M(T_E < \infty) = \mathbb{P}_W(T_{\psi(E)} < \infty), \forall E \in \mathcal{B}^*(X). \quad (3)$$

Proof. Since H and H' are bisimilar w.r.t. $\mathcal{R} \subset X \times Y$ then the processes M and W are bisimilar, i.e. their capacities are equivalent: $Cap_M(\pi_X^{-1}(A)) = Cap_W(\pi_Y^{-1}[\psi(A)])$ (for all $A \in \mathcal{B}(X/_\mathcal{R})$), where ψ is the homeomorphism induced by the measurable relation $\mathcal{R}$. If $E \in \mathcal{B}^*(X)$ (saturated w.r.t. $\mathcal{R}$), then it can be seen as an element of $\mathcal{B}(X/_\mathcal{R})$ and we

have $E = \pi_X^{-1}(E)$; $\psi(E) = \pi_Y^{-1}[\psi(E)$. This implies the following equality

$$Cap_M(E) = Cap_W([\psi(E)]). \quad (4)$$

From (4) and the formula of a Markov process capacity (1) we get the equality (3) of the reach set probabilities corresponding to the saturated target set E.□

The Prop.6 shows that our definition of bisimulation between stochastic hybrid systems is natural since the probabilities of the reachable events are preserved. Then naturally, the reachability analysis of a stochastic hybrid system can be performed using much simpler stochastic hybrid systems bisimilar with the given one.

V. Final remarks

Bisimulation of hybrid systems is a recent research subject actively investigated. The pioneering work of Tabuada, Pappas e.a. (see references from [25]) was used to investigate model checking of control and hybrid systems [26]. For stochastic hybrid systems, Van der Schaft and coworkers [24] investigated bisimulation for the first time. The later approach is based on weight function and piecewise deterministic Markov processes. Reachability analysis is a traditional problem for timed systems. It has been investigated for hybrid systems since the time of their birth. The stochastic case has been investigated very recently [18], [1], [3], [4]. Bisimulations were applied to reachability analysis, in the context of hybrid systems, for the first time in [17]. An inductive continuation of this trend is to use bisimulations to reachability analysis for stochastic hybrid systems. This is the subject of this paper.

The approach we have presented is dependable, in the sense that the probabilities can be recalculated as the system evolves, offering assistance for decision making in a dynamic, configurable change prone environment. Moreover, we could consider a probabilistic version of model checking, meaning that one could get a system abstraction (hopefully simpler or even finite state) that preserves the probabilities. This technique requires a suitable concept of bisimulation. In this paper we have presented a stochastic bisimulation concept and proved that two bisimilar processes have the same probabilities of reach a safety critical (hazardous) situation - called reach set probabilities. The bisimulation concept is very robust because it is not based on the equality of transition probabilities. In practice probabilities are approximated by various statistical methods and therefore equality of transition probabilities is difficult to be checked. In this context, the preservation of reach set probabilities is major breakthrough result towards applying model checking to reachability analyisis. Then, a model-checking algorithm might be further developed in a future work. In this paper we focus only on the theoretical foundations that make possible the probabilistic model checking.

References

[1] Bayen A., Cruck E., Tomlin C.: *Guaranteed Overapproximations of Unsafe Sets for Continuous and Hybrid Systems: Solving the Hamilton-Jacobi Equation Using Viability Techniques* Springer-Verlag LNCS series, Vol. 2289, (2002).

[2] Bernadskiy, M., Sharykin, R., Alur, R.: *Structured Modelling of Concurrent Stochastic Hybrid Systems*. Joint Conference on Formal Modelling and Analysis of Time Systems and Formal Techniques in Real-Time and Fault Tolerant Systems, 2004.

[3] Bujorianu, M.L., Lygeros, J.: *Reachability Questions in Piecewise Deterministic Markov Processes*. In O. Maler, A. Pnueli Eds., *Hybrid Systems: Computation and Control*, 6th International Workshop, HSCC03, LNCS 2623 (2003), 126-140.

[4] Bujorianu M.L : *Extended Stochastic Hybrid Systems and their Reachability Problem*. In R. Alur, G. Pappas Eds., *Hybrid Systems: Computation and Control* 7th International Workshop, HSCC04, Springer LNCS 2993 (2004), 234-249.

[5] Bujorianu, M.L., Lygeros, J., Bujorianu, M.C.: *Bisimulation for General Stochastic Hybrid Systems*. To appear in M. Morari, L. Thiele Eds., *Hybrid Systems: Computation and Control* 8th International Workshop, HSCC04, Springer LNCS 4314 (2005), 198-214.

[6] Choquet, G.: *Theory of Capacities*. Annales de l'Institut Fourier, Grenoble, **5** (1953), 131-291.

[7] Davis, M.H.A.: "*Markov Models and Optimization*", Chapman & Hall, London (1993).

[8] Dempster, D.: *Upper and Lower Probabilities Induced by a Multivalued Mapping*. Ann. Math. Statist. **38** (1967), 325-339.

[9] Dubois, D., Prade, H.: *Modelling Uncertainty and Inductive Inference: A Survey of Recent Non-Additive Probability Systems*. Acta Psychologica **68** (1988), 53-78.

[10] Epstein, L.G., Wang, T.: *Intertemporal Asset Pricing under Knightian Uncertainty*. Econometrica **62** (1994), 283-322.

[11] Fine, T.L.: *Lower Probability Models for Uncertainty and nondeterministic Processes*. J. Statist. Plann. Inference **20** (1988), 389-411.

[12] Fitzsimmons, P.J.: *Markov Processes with Equal Capacities.* J. Theor. Prob. **12** (1999), 271-292.

[13] Getoor, R.K.: Excessive Measures. Birkhäuser, Boston, 1990.

[14] Huber, P.J., Strassen, V.: *Minimax Tests and the Neyman-Pearson Lemma for Capacities*. Ann. of Statist. **1** (1973), 251-263.

[15] Hespanha J.: *Stochastic Hybrid Systems: Theory and Applications*. Workshop for the 43rd IEEE Conference on Decision and Control, December 2004.

[16] Huber, P.J.: "Robust Statistics". Willey, New York, 1980.

[17] Lafferriere G., Pappas G.J., Sastry S.: *Reachability analysis of hybrid systems using bisimulations* Proceedings of the 37th IEEE Conference on Decision and Control, pages 1623-1628, Tampa, 1998

[18] Lygeros J., Tomlin C., Sastry S.: *Controllers for Reachability Specifi - cations for Hybrid Systems* Automatica, Volume 35, Number 3, March 1999.

[19] Meyer, P.A.: **"***Processus de Markov*". LNM., **26**, Springer Verlag, Berlin, (1976).

[20] G. Pola, Bujorianu, M.L., Lygeros, J., Di Benedetto, M. D.: *Stochastic Hybrid Models: An Overview with applications to Air Traffi c Management.* Proccedings Analysis and Design of Hybrid Systems IFAC ADHS03, 45-50, 2003.

[21] Richard, B., Desharnais, J., Edalat, A., Panangaden, P.: *Bisimulation for Labelled Markov Processes.* In Logic in Computer Science, IEEE Press (1997), 149-158.

[22] Shafer, G.: "*A Mathematical Theory of Evidence*". Princeton University Press, Princeton, New Jersey, 1976.

[23] Schmeidler, D.: *Subjective Probability and Expected Utility Without Additivity*. Econometrica **57** (1989), 571-587.

[24] Schaft, A.J. van der: *Bisimulation of Dynamical Systems*. In R. Alur, G. Pappas Eds., Hybrid Systems: Computation and Control 7th International Workshop, HSCC 2004, Springer LNCS 2993, 559-569.

[25] Tabuada P., Pappas G.J., Lima P.: *Compositional Abstractions of Hybrid Control Systems* Journal of Discrete Event Dynamical Systems, 14(2), 203-238, April 2004.

[26] Tabuada P., PappasG.J.: *Model Checking LTL over Controllable Linear Systems is Decidable* In Hybrid Systems: Computation and Control, Springer-Verlag LNCS 2623, 2003.

[27] Viertl, R.: "*Statistical Methods for Non-Precise Data*". CRC Press, Boca Raton, Florida (1996).

[28] Walley, P.: "*Statistical Reasoning with Imprecise Probabilities*". Chapman and Hall, London (1991).