12-9-2008

Probabilistic Testing for Stochastic Hybrid Systems

A. Agung Julius
University of Pennsylvania, agung@seas.upenn.edu

George J. Pappas
University of Pennsylvania, pappasg@seas.upenn.edu

Probabilistic Testing for Stochastic Hybrid Systems

Abstract
In this paper we propose a testing based method for safety/ reachability analysis of stochastic hybrid systems. Testing based methods are characterized by analysis based on the execution traces of the system or the simulation thereof. Testing based method is very appealing because of the simplicity of its execution, the possibility of having a partial verification, and its highly parallel structure. The key idea in this paper is the construction of a robust neighborhood consisting of states that have the same probabilistic safety/reachability properties. We construct the robust neighborhood using the level sets of a stochastic bisimulation function. We also show how to construct stochastic bisimulation functions for systems whose continuous dynamics is stable and linear. As a case example, we consider the problem of conflict detection of aircraft flight, and show that we can infer some robust probabilistic safety property by using the algorithm that we present in this paper.

Keywords
probability, reachability analysis, stochastic systems, probabilistic safety property, probabilistic testing, reachability property, robust neighborhood concept, stochastic bisimulation function, stochastic hybrid system, testing based method

Comments
Copyright 2008 IEEE. Reprinted from:

Julius, A.A.; Pappas, G.J., "Probabilistic testing for stochastic hybrid systems," Decision and Control, 2008. CDC 2008. 47th IEEE Conference on , vol., no., pp.4030-4035, 9-11 Dec. 2008

URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4739166&isnumber=4738560

Proceedings of the
47th IEEE Conference on Decision and Control
Cancun, Mexico, Dec. 9-11, 2008

Probabilistic Testing for Stochastic Hybrid Systems

A. Agung Julius and George J. Pappas

Abstract— **In this paper we propose a testing based method for safety/ reachability analysis of stochastic hybrid systems. Testing based methods are characterized by analysis based on the execution traces of the system or the simulation thereof. Testing based method is very appealing because of the simplicity of its execution, the possibility of having a partial verification, and its highly parallel structure.**

The key idea in this paper is the construction of a robust neighborhood consisting of states that have the same probabilistic safety/reachability properties. We construct the robust neighborhood using the level sets of a stochastic bisimulation function. We also show how to construct stochastic bisimulation functions for systems whose continuous dynamics is stable and linear. As a case example, we consider the problem of conflict detection of aircraft flight, and show that we can infer some robust probabilistic safety property by using the algorithm that we present in this paper.

I. Introduction

As safety verification and reachability analysis of hybrid systems become more complicated, new formal verification concepts are needed. Testing based verification has emerged as an alternative way to perform such task [1]. By testing based verification, we mean the analysis methods that are based on the execution traces of the system or the simulation thereof. Each test run is characterized by a *test parameter*. The totality of test parameters in a testing problem is called the *test parameter space*. For example, in a safety verification problem, where it is desired to verify the safety of all executions that start from a certain set of initial states, each test run is characterized by its initial condition. The test parameter space is thus the set of initial conditions.

Testing based verification is very appealing because of several reasons. The first reason is its simplicity. Running or simulating the execution traces of a system is generally much simpler than performing symbolic analysis on it. This is particularly true for systems with complex dynamics. The second reason is that when coupled with an appropriate notion of coverage, testing can lead to *partial verification*. It is generally known that when a to-be-verified system does not robustly satisfy the desired property, the complexity of its full verification becomes prohibitively high [2]. Testing based safety verification can, for example, provide a safety guarantee for a subset of the initial conditions that is robustly safe after only executing a few runs. Therefore, if we decide to conclude the testing procedure after a finite time, we can still obtain a partial verification of the system. Another reason why testing based verification is attractive is that its algorithm is highly parallelizable. Since simulations of execution of the system do not depend one on another, they can be easily assigned to different processors, resulting in a highly parallel system.

Since there are infinitely many possible execution traces of a hybrid system, a necessary question that a testing based verification method needs to answer is how to generalize formally the results based on finitely many execution traces to the whole system. We address this question by introducing a concept of test run robustness [1]. A test run is robust if it shares the same properties as other test runs that are close to it. Distance between test runs is defined as the distance between their test parameters. Obviously, if a test run is robust, it can be used as a representative of a neighborhood of (infinitely many) test runs around it. When a system robustly satisfies a desired property, every test run also robustly satisfies the property. As a result, if the space of test parameters is compact, the system can be verified to satisfy the property by using finitely many test runs.

Trajectory based verification methods have already been previously used in verification of hybrid and dynamical systems. For example, there is quite a big research effort in trajectory sampling based methods [3], [4], [5], [6], [7], [8], [9], [10]. The work presented in this paper differs with most of the references above in that (1) we do not discretize the execution trajectories, and (2) we work with a probabilistic notion of safety for stochastic systems. Several other methods have been developed for analysis of stochastic hybrid systems, for example, based on statistical moments computation [11], discretization into Markov chains [12], [13], and construction of barrier functions [14]. The approach that we propose in this paper is very different from the previous approaches, in the sense that we are able to infer some reachability/safety property of the system by using the trajectory of the diffusionless version of the process corresponding to the stochastic hybrid system. We also apply the proposed method to an case example of conflict detection in aircraft flight.

II. Mathematical preliminary

A. Modeling formalism

In this paper we model stochastic hybrid systems as a 5-tuple, $\mathcal{H} = (\mathcal{X}, \mathcal{L}, E, Inv, Dyn)$, where $\mathcal{X}$ is the continuous state space of the system, $\mathcal{L}$ is the finite state of discrete states (locations), E is the set of transitions, $Inv : \mathcal{L} \rightarrow 2^{\mathcal{X}}$ is the invariant set of a location, and $Dyn(l)$ is a set of stochastic differential equations (SDE) that describes the continuous dynamics in location $l \in \mathcal{L}$.

A transition $e \in E$ is a 4-tuple (l, l', g, r), where $l \in \mathcal{L}$ is the origin of the transition, $l' \in \mathcal{L}$ is the target of the transition and that each location, $g \subset \partial Inv(l)$ is the guard of the transition, which is a subset of the boundary of the invariant set of location l, and $r : g \rightarrow Inv(l')$ is the reset

This work is partially funded by National Science Foundations awards CSR-EHS 0720518 and CSR-EHS 0509327.

The authors are with the Dept. Electrical and Systems Engineering, University of Pennsylvania, 3330 Walnut Street, Philadelphia, PA 19104, U.S.A. agung,pappasg@seas.upenn.edu

map that resets the continuous state at the new location. We assume that the reset map r is deterministic and continuous.

In this paper, we adopt the following assumptions:

- the continuous state space is $\mathbb{R}^n$,
- the invariant sets are open,
- the stochastic differential equations that describe the continuous dynamics in every location is *well posed* (more detailed assumptions are given in the following section),
- the stochastic hybrid systems as stochastic processes are *cadlag* (the realizations are right continuous with limit from the left),
- the guards of all outgoing transitions from a location are disjoint,
- there is a subset $Unsafe \subset \mathcal{X} \times \mathcal{L}$ of unsafe states. A trajectory of the hybrid system corresponds to an unsafe execution if it intersects with the unsafe set.

B. Finite time stochastic bisimulation and stability

Define a system given by a family of independent stochastic processes, which is indexed by the initial condition.

$$\xi_{x,t} : d\xi_{x,t} = F(\xi_{x,t})dt + G(\xi_{x,t})dw_t,\ \xi_{x,0} = x \in \mathcal{X}, \quad (1)$$

where w_t is an $\mathbb{R}^m-$valued standard Brownian motion. To guarantee the existence and uniqueness of the solution of (1), we assume that [15]

- F and G are locally Lipschitz: For any $R \in \mathbb{R}_+$, there exists a $K(R) \in \mathbb{R}_+$ such that

$$\|x_1\|, \|x_2\| \leq R \Rightarrow$$
$$\|F(x_1) - F(x_2)\| + \|G(x_1) - G(x_2)\| \leq K(R).$$

- F and G satisfy linear growth condition: There exists a K' such that for all $x \in \mathcal{X}$,

$$\|F(x)\| + \|G(x)\| \leq K'(1 + \|x\|).$$

We define the **nominal system** of (1), $\xi^*_{x,t}$, as the diffusionless version given by

$$\xi^*_{x,t} : d\xi^*_{x,t} = F(\xi^*_{x,t})dt,\ \xi^*_{x,0} = x \in \mathcal{X}. \quad (2)$$

Notice that (2) defines an ordinary differential equation. Moreover, due to Lipschitz assumption above, (2) admits a unique solution for every initial condition $x \in \mathcal{X}$. The trajectories of the nominal system are called **nominal trajectories**.

The nominal system (2) can be thought of as a deterministic approximation of the real system (1). To compute a bound on the quality of the approximation, we establish a notion of finite time stochastic bisimulation. This is a generalization of our previous work in stochastic bisimulation [16], [17].

Definition 2.1: A twice differentiable function $\phi : \mathcal{X} \times \mathcal{X} \to \mathbb{R}_+$ is a **finite time stochastic bisimulation function** between (1) and its nominal system (2) if it satisfies

$$\phi(x_1, x_2) \geq \|x_1 - x_2\|^2, \forall x_1, x_2 \in \mathcal{X}, \quad (3)$$
$$\phi(x, x) = 0, \forall x \in \mathcal{X}, \quad (4)$$

and there exist $\mu, \alpha > 0$ such that

$$\frac{\partial \phi}{\partial x_1}F(x_1) + \frac{\partial \phi}{\partial x_2}F(x_2) + \frac{1}{2}Tr\left(G^T(x_1)\frac{\partial^2 \phi}{\partial x_1^2}G(x_1)\right) \leq -\mu\phi + \alpha, \quad (5)$$

for any $x_1, x_2 \in \mathcal{X}$. The smallest α that satisfies (5) is called the **bias** of ϕ.

The role of finite time stochastic bisimulation function in establishing a bound on the quality of the approximation is given in the following proposition.

Proposition 2.2: ([18] Chapter III) Given a finite time stochastic bisimulation function $\phi(\cdot, \cdot)$ between (1) and its nominal system (2), the following relation holds.

$$P\left\{\sup_{0 \leq t \leq T} \phi(\xi_{x,t}, \xi^*_{x,t}) \geq m\right\} \leq \frac{\alpha T}{m}, \forall T > 0. \quad (6)$$

Recalling that $\phi(\cdot, \cdot)$ is an upper bound for the square of the distance between the states, we can conclude that Proposition 2.2 provides a probabilistic upper bound for the distance between the states in a finite time horizon.

Notation. We denote the level sets of ϕ as

$$B_\phi(x, r) := \{x' \in \mathcal{X} \mid \phi(x, x') = \phi(x', x) \leq r\}, \forall r \geq 0. \quad (7)$$

C. Review on bisimulation of deterministic systems

Define a deterministic system by an ordinary differential equation as:

$$\frac{dx}{dt} = F(x), x \in \mathcal{X}, \quad (8)$$

where F satisfies the locally Lipschitz and linear growth condition as mentioned in the previous subsection. A differentiable function $\gamma : \mathcal{X} \times \mathcal{X} \to \mathbb{R}_+$ is a **bisimulation function** of the deterministic system if $\forall (x_1, x_2) \in \mathcal{X} \times \mathcal{X}$,

$$\frac{\partial \gamma(x_1, x_2)}{\partial x_1}F(x_1) + \frac{\partial \gamma(x_1, x_2)}{\partial x_2}F(x_2) \leq 0. \quad (9)$$

The idea of bisimulation function stems from the seminal work of Girard and Pappas [19], [20]. We have used this idea for developing a robust testing framework for deterministic hybrid systems [1].

From (9), it follows that $\gamma(x_1(t), x_2(t))$ is monotonically nonincreasing, for any trajectories $x_1(t)$ and $x_2(t)$ of the system. This leads to the following corollary.

Corollary 2.3: Given a system (8) and a bisimulation function $\gamma(\cdot, \cdot)$, for any two initial conditions $x_0, x'_0 \in \mathcal{X}$, the trajectories originating from these states, $x(t)$ and $x'(t)$ satisfy $\gamma(x(t), x'(t)) \leq \gamma(x_0, x'_0)$.

D. Bisimulation functions as pseudometrics

In this paper, we combine the upper bounds provided by the finite time stochastic bisimulation function and the deterministic bisimulation function to form a notion of robustness for the nominal trajectories of a stochastic hybrid system. The idea is to define both bisimulation functions as pseudometrics. From there, it follows that Proposition 2.2 and Corollary 2.3 provide some bounds on how far the trajectories of the original system and the nominal system (Proposition 2.2), or two trajectories of the nominal system (Corollary 2.3) can diverge.

Assumption: In this paper, we assume that finite time stochastic bisimulation functions and deterministic bisimulation functions are pseudometrics. That is, they are nonnegative, symmetric, and satisfy the triangular inequality

$$f(x, z) \leq f(x, y) + f(y, z), \forall x, y, z \in \mathcal{X}. \quad (10)$$

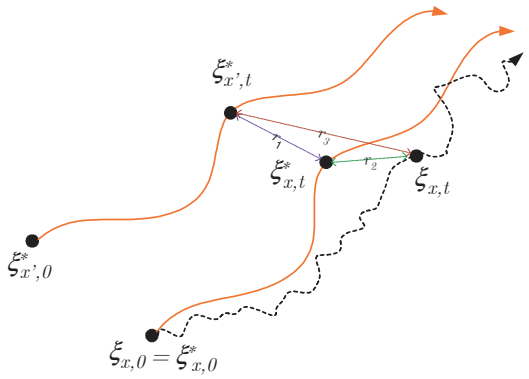

Fig. 1. An illustration for Theorem 3.1. We construct a (probabilistic) bound for the distance between $\xi^*_{x',t}$ and $\xi_{x,t}$ (shown as r_3) through the bounds on r_1 (provided by Proposition 2.2) and r_2 (provided by Corollary 2.3).

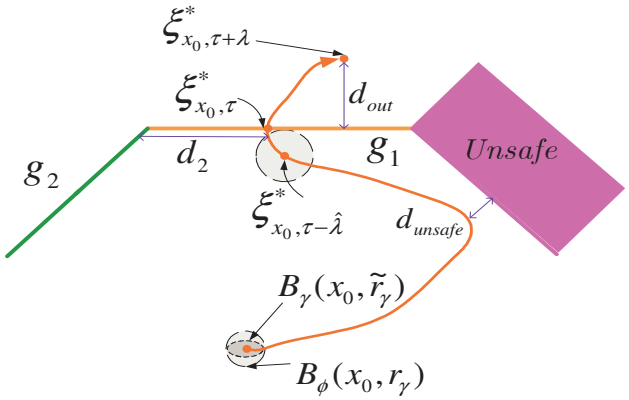

Fig. 2. An illustration for Proposition 3.2. The trajectory shown here is $\xi^*_{x_0,t}$, the nominal trajectory starting at x_0. The circle that touches the guard g_1 is the ball $B_\phi(\xi^*_{x_0,\tau-\hat{\lambda}}, d_{\min})$. Proposition 3.2 provides a probabilistic guarantee that any initial condition in $B_\phi(x_0,\tilde{r}_\gamma)$ will result in a stochastic realization with the same qualitative property as the nominal trajectory.

Naturally, we can also define balls with respect to the pseudometrics, which are denoted as

$$B_\phi(x,r) := \{x' \in \mathcal{X} \mid \phi(x,x') \leq r\}, \forall x \in \mathcal{X}, r \geq 0. \quad (11)$$

III. Probabilistic Testing of Stochastic Hybrid Systems

A. Probabilistic robustness of nominal trajectories

Consider the system $\xi_{x,t}$ as given by (1), and its nominal system $\xi^*_{x,t}$ as given by (2). We are going to use the results in Proposition 2.2 and Corollary 2.3 to establish a notion of probabilistic robustness for the trajectories of the nominal system with respect to the trajectories of the original system.

Theorem 3.1: Given a finite time stochastic bisimulation function $\phi(\cdot,\cdot)$ between $\xi_{x,t}$ and its nominal system $\xi^*_{x,t}$, and a bisimulation function $\gamma(\cdot,\cdot)$ of $\xi^*_{x,t}$, the following relation holds for any $x, x' \in \mathcal{X}$ and $T > 0$

$$P\left\{\sup_{0\leq t\leq T} \phi\left(\xi_{x,t}, \xi^*_{x',t}\right) \geq m + \lambda\right\} \leq \frac{\alpha T}{m}, \quad (12)$$

where

$$\lambda := \sup_{z\in\mathcal{X}} \sup_{z'\in B_\gamma(z,\gamma(x,x'))} \phi(z,z'). \quad (13)$$

Safety verification typically amounts to verifying the a system's trajectories do not enter a set of states that are declared unsafe [21]. Theorem 3.1 is one of the key ideas in this paper. Basically, it allows us to (1) establish a probabilistic safety guarantee for an initial condition for a finite time horizon and (2) extend the guarantee to a neighborhood around the initial condition.

The extension of this result to stochastic hybrid systems is quite straightforward and analogous to its deterministic counterpart in [1].

Notation. For any location $l \in \mathcal{L}$ we define the set of outgoing transitions from l as $Out(l)$. The continuous dynamics in a location $l \in \mathcal{L}$ is described by the stochastic differential equation

$$d\xi_{x,t} = F_l(\xi_{x,t})dt + G_l(\xi_{x,t})dw_t. \quad (14)$$

Proposition 3.2: Let $x_0 \in Inv(l)$ for some location $l \in \mathcal{L}$, and $\xi^*_{x_0,t}$ be the trajectory of the nominal system of (14) with initial condition x_0. Suppose that:

- $\xi^*_{x_0,t}$ lies entirely in $Inv(l)\backslash Unsafe$ for $t \leq \tau$,
- $\phi(\cdot,\cdot)$ is a finite time stochastic bisimulation function for the stochastic dynamics in location l,
- $\gamma(\cdot,\cdot)$ is a deterministic bisimulation function for the nominal system in location l with bias α,
- $Out(l) = \{e_1, e_2, \cdots, e_n\}$ and g_i is the guard of e_i, $i = 1,\ldots,n$,
- τ is the time when $\xi^*_{x_0,t}$ hits g_1, which is the guard of a transition e_1, and
- there is a positive time lag $\lambda > 0$ such that $\xi^*_{x_0,\tau+\lambda} \notin Inv(l)$.

We define

$$\begin{aligned}
d_{\text{out}} &:= \inf_{y\in g_1} \phi(\xi^*_{x_0,\tau+\lambda}, y),\\
d_i &:= \inf_{0\leq t\leq \tau+\lambda} \inf_{y\in g_i} \phi(\xi^*_{x_0,t}, y), i = 2,3,\ldots,n,\\
d_{\text{unsafe}} &:= \inf_{0\leq t\leq \tau+\lambda} \inf_{y\in Inv(l)\cap Unsafe} \phi(\xi^*_{x_0,t}, y),\\
d_{\min} &:= \min\{d_{\text{out}}, d_{\text{unsafe}}, d_2, d_3, \cdots d_n\},\\
\hat{\lambda} &:= \inf\left\{\delta > 0 \mid B_\phi(\xi^*_{x_0,\tau-\delta}, d_{\min}) \subset Inv(l)\right\}.
\end{aligned}$$

For any $\rho, \varepsilon > 0$, such that

$$\rho + \varepsilon = d_{\min}, \quad (15)$$

define

$$\tilde{\rho} := \sup_{z\in\mathcal{X}} \sup_{z'\in B_\phi(z,\rho)} \gamma(z,z'). \quad (16)$$

The following statement holds. For any $x'_0 \in B_\gamma(x_0,\tilde{\rho})$, the stochastic process $\xi_{x'_0,t}$ exits $Inv(l)$ through transition e_1 at time $t \in [\tau-\hat{\lambda}, \tau+\lambda]$ and is safe at least until it exits location l with probability greater than $\left(1 - \frac{\alpha(\tau+\lambda)}{\varepsilon}\right)$.

Proposition 3.2 enables us to compute a neighborhood around the initial state x_0, consisting of initial states that lead to realizations have the same qualitative behavior as $\xi^*_{x_0,t}$ with some probability bound. By the same qualitative

property we mean the realizations that exits the location l by performing the same transition, and is safe at least until it performs the transition. In addition to that, we also obtain a timing guarantee, in the form of a time interval $[\tau - \hat{\lambda}, \tau + \lambda]$ where the transition is guaranteed to occur, with some probability bound, if the initial state is varied within the computed neighborhood.

Remark 3.3: Notice that in (15), we split $d_{\min}$ into ε and ρ. The bigger ρ is, the larger the robust neighborhood that we compute. On the other hand, the bigger ε is, the higher is the confidence provided by the guarantee. Thus, we have a trade-off between the size of the robust neighborhood and the confidence level that is provided by the guarantee.

B. Probabilistic testing algorithm

In this subsection we design an algorithm that uses Proposition 3.2 repetitively to deal with nominal trajectories with multiple transitions. The purpose of the algorithm can be explained as follows. Given a stochastic hybrid system $\mathcal{H} = (\mathcal{X}, \mathcal{L}, E, Inv, Dyn)$, an initial state $(x_0, l_0) \in Inv(l_0) \times \mathcal{L}$, and the hybrid nominal trajectory starting from (x_0, l_0), we want to compute a robust neighborhood around that initial state. A hybrid nominal trajectory is a trajectory of the deterministic hybrid system constructed by changing the stochastic continuous dynamics in $\mathcal{H}$ with their nominal systems. A nominal trajectory can be obtained through numerical simulation of the nominal system, and it constitutes a test. The overall goal is to generate and analyze many tests so as to cover a set of initial states $X_0 \subset \mathcal{X} \times \mathcal{L}$.

Denote the nominal trajectory starting from (x_0, l_0) as the sequence $(\zeta_i, l_i, e_i, \tau_i)_{i=0,\cdots,N}$, where $\zeta_0(0) = x_0$ and for every $i \in \{0, 1, \ldots N\}$,

- $l_i \in L$ and $e_i \in Out(l_i), \tau_i > 0$,
- $\zeta_i(t)$ is a nominal trajectory of the dynamics in location l_i,
- $\zeta_i(t) \in Inv(l_i)$, for $t \in [0, \tau_i)$,
- For every $i \in \{0, 1, \ldots N-1\}$, if we define $e_i = (l_i, l_{i+1}, g_i, r_i)$, then $\zeta_i(\tau_i) \in g_i$, $\zeta_{i+1}(0) = r_i(\zeta_i(\tau_i))$.

We define $T := \sum_{i=0}^{N-1} \tau_i$, which is the time where the trajectory enter the final state. The length of the test is $T + \tau_N$. We assume that for each location $l_i \in L$, we have a finite time stochastic bisimulation function $\phi_i(\cdot,\cdot)$ with bias α_i, and a deterministic bisimulation function $\gamma_i(\cdot,\cdot)$ for the nominal system. Given a realization sequence $(\zeta_i, l_i, e_i, \tau_i)_{i=0,\cdots,N}$, and a sequence $(\varepsilon_i)_{i=0,\cdots,N} > 0$, the algorithm for constructing a robust neighborhood around the initial state is given in Algorithm 1[1].

The result of this iteration have the following property.

Theorem 3.4: Given a realization sequence $(\zeta_i, l_i, e_i, \tau_i)_{i=0,\cdots,N}$, let $(\varepsilon_i)_{i=0,\cdots,N} > 0$, $(\rho_i)_{i=0,\cdots,N} > 0$, $(\tilde{\rho}_i)_{i=0,\cdots,N} > 0$, $d_{\min,i}$, λ_i, $\hat{\lambda}_i$, $i = 0, 1, \ldots, N-1$ be obtained from the iteration in Algorithm 1. Define

$$\lambda := \sum_{i=0}^{N-1} \lambda_i, \ \hat{\lambda} := \sum_{i=0}^{N-1} \hat{\lambda}_i.$$

[1]Notice that for simplicity, we abuse the notation and associate the transition with its guard.

Algorithm 1 Computation of probabilistic robust neighborhood for hybrid nominal trajectories

Require: A nominal trajectory starting from (x_0, l_0) as the sequence $(\zeta_i, l_i, e_i, \tau_i)_{i=0,\cdots,N}$

1: Define the avoided set as the union of the unsafe set and all outgoing guards from l_N, i.e.

$$D_N := Unsafe \cup_{g \in Out(l_N)} g. \tag{17}$$

2: Compute (or obtain a lower bound on)

$$d_{\min,N} := \inf_{t \le \tau_N} \inf_{y \in D_N} \phi_N(\zeta_N(t), y). \tag{18}$$

3: Define $\lambda_N = 0$, and ε_i,$\rho_i, \tilde{\rho}_i > 0$ such that

$$\varepsilon_N + \rho_N = d_{\min,N}, \tag{19}$$

$$\tilde{\rho}_N := \sup_{z \in \mathcal{X}} \sup_{z' \in B_{\phi_N}(z, \rho_N)} \gamma_N(z, z') \tag{20}$$

4: **for** i=N to 1 **do**

5: Define ε_i,$\rho_i, \tilde{\rho}_i > 0$ such that

$$\varepsilon_i + \rho_i = d_{\min,i}, \tag{21}$$

$$\tilde{\rho}_i := \sup_{z \in \mathcal{X}} \sup_{z' \in B_{\phi_i}(z, \rho_i)} \gamma_i(z, z') \tag{22}$$

6: Define the allowed guard

$$W_{i-1} := r_{i-1}^{-1}(r_{i-1}(g_{i-1}) \cap B_{\gamma_i}(\zeta_N(0), \tilde{\rho}_i)). \tag{23}$$

This is the set of states on the guard of the transition between l_{i-1} and l_i that is reset into $B_{\phi_i}(\zeta_N(0), \tilde{\rho}_i)$.

7: Define the avoided set

$$D_{i-1} := (Unsafe \cup_{g \in Out(l_{i-1})} g) \backslash W_{i-1}. \tag{24}$$

8: Continue the trajectory $\zeta_{i-1}(t)$ beyond $t = \tau_{i-1}$. Pick a time lag $\lambda_{i-1} > 0$ such that

$$\zeta_{i-1}(\tau_{i-1} + \lambda_{i-1}) \notin Inv(l_{i-1}).$$

9: Compute (or obtain a lower bound on)

$$d_{\min,i-1} := \min \left(\inf_{y \in g_{i-1}} \phi_{i-1}(\zeta_{i-1}(\tau_{i-1} + \lambda_{i-1}), y), \right.$$
$$\left. \inf_{t \le \tau_{i-1} + \lambda_{i-1}} \inf_{y \in D_{i-1}} \phi_{i-1}(\zeta_{i-1}(t), y) \right).$$

10: Define

$$\hat{\lambda}_{i-1} := \sup \{\delta > 0 \mid B_{\phi_{i-1}}(\zeta_{i-1}(\tau_{i-1} - \delta), d_{\min,i-1}) \not\subset Inv(l_{i-1})\}.$$

11: **end for**

For any $x_0' \in B_{\gamma_0}(x_0, \tilde{\rho}_0)$, the stochastic hybrid trajectories with initial state (x_0', l_0) satisfy the following properties with probability larger than $\prod_{i=0\ldots N}\left(1-\frac{\alpha_i(\tau_i+\lambda_i)}{\varepsilon_i}\right)$.
(a) They follow the same sequence of locations, $(l_i)_{i=0,\ldots,N}$ and enter the final location l_N at $t \in [T-\hat{\lambda}, T+\lambda]$.
(b) The trajectories are safe at least until τ_N time unit after it enters l_N.

C. Construction of stochastic bisimulation functions for stable linear affine dynamics

In this subsection we present a construction of the finite time stochastic bisimulation function and deterministic bisimulation function for a special class of stochastic processes, namely, those with stable linear affine dynamics. The method of construction is similar to that presented in our earlier work [16], [1], where they are used in constructing an approximate abstraction for stochastic and deterministic hybrid systems. We shall use this construction in testing the example in the following section.

We consider the construction of stochastic bisimulation functions for the family of stochastic processes $\xi_{x,t}$ given by the stochastic differential equation

$$\xi_{x,t} : d\xi_{x,t} = (A\xi_{x,t} + B)dt + \Sigma dw_t,\ \xi_{x,0} = x \in \mathcal{X}, \quad (25)$$

with $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times 1}$, and $\Sigma \in \mathbb{R}^{n\times m}$. Furthermore, we assume that A is Hurwitz. This means that the eigenvalues of A have negative real parts and the dynamics described by the drift term is stable.

Consider a function of the form

$$\phi(x_1, x_2) = (x_1 - x_2)^T M (x_1 - x_2), \quad (26)$$

where M is a symmetric positive definite matrix. In order for this function to qualify as a finite time stochastic bisimulation function, we need to have (see (3) - (5)) $M > I$, and

$$\begin{aligned}
&\frac{\partial \phi}{\partial x_1}(Ax_1 + B) + \frac{\partial \phi}{\partial x_2}(Ax_2 + B) + \\
&\quad + \frac{1}{2} Tr\left(\Sigma^T \left(\frac{\partial^2 \phi(x_1, x_2)}{\partial x_1^2}\right)\Sigma\right) \\
&= 2(x_1 - x_2)^T M A (x_1 - x_2) + Tr(\Sigma^T M \Sigma), \\
&\leq -\mu (x_1 - x_2)^T M (x_1 - x_2) + \alpha, \quad (27)
\end{aligned}$$

for some $\mu, \alpha > 0$. If we pick $\alpha = Tr(\Sigma^T M \Sigma)$, the inequality (27) becomes a linear matrix inequality (LMI)

$$A^T M + MA + \mu M \leq 0. \quad (28)$$

Inequality (28) is a Lyapunov inequality, and we can construct such an M for any μ small enough such that $\left(A + \frac{\mu}{2} I\right)$ is Hurwitz [22].

Based on (9), we can also verify that $\phi(x_1, x_2) = (x_1 - x_2)^T M (x_1 - x_2)$ constructed as above, is also a deterministic bisimulation function for the nominal system

$$\xi^*_{x,t} : \frac{d}{dt}\xi^*_{x,t} = (A\xi_{x,t} + B). \quad (29)$$

Thus constructing a stochastic bisimulation function here involves solving a Lyapunov LMI (28). This type of problems is standard in systems and control theory, and there are a number of software packages that can be used to solve them, such as YALMIP [23] and `cvx` [24].

IV. Example: Conflict detection in aircraft flight

In this section, we apply our framework in conflict detection in aircraft flight. The problem of conflict detection can be described as assessing the conflict probability of two or more aircraft, given their flight plan. Conflict means an aircraft entering a forbidden zone, which typically means that the aircraft is dangerously close to another aircraft [25], [12]. We adopt a simple model for aircraft flight, inspired by the model presented in [12].

We model each aircraft as point mass moving on a plane of constant altitude[2]. Each aircraft follows a sequence of waypoints in such a way that the dynamics of its motion is switched every time a waypoint is reach so that the aircraft then proceed to the next waypoint. This switching behavior makes the dynamics hybrid. Moreover, because of uncertain environmental factors such as wind, the dynamics is also stochastic.

The continuous states of an aircraft are given by its planar coordinates and their respective velocities. The discrete state is defined by the waypoint that it is headed to. For simplicity, we adopt a linear affine model

$$d\xi_t = (A_i \xi_t + B_i)dt + W_i dw_t \quad (30)$$

for the continuous stochastic dynamics for the aircraft headed to waypoint i. Here we have

$$A_i = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -10 & 0 & -10 & 0 \\ 0 & -10 & 0 & 10 \end{bmatrix}, B_i = \begin{bmatrix} v_{x,i} \\ v_{y,i} \\ 10{\cdot}p_{x,i} \\ 10{\cdot}p_{y,i} \end{bmatrix}, W_i = \begin{bmatrix} 0 \\ 0 \\ \omega_{x,i} \\ \omega_{y,i} \end{bmatrix}. \quad (31)$$

The vector $[v_x\ v_y]$ is an offset velocity vector pointing from waypoint $i-1$ to waypoint i, the vector $[p_x\ p_y]$ is the coordinate of waypoint i, and $[\omega_x\ \omega_y]$ indicates the direction of wind perturbation. We also assume that the aircraft will switch to the next waypoint $(i+1)$ if it has crossed a vertical plane that passes through its current waypoint. Thus the transition guard can be given by a half space

$$g_i = \{x \in \mathbb{R}^4 | a_1 x_1 + a_2 x_2 \leq b\}, \quad (32)$$

for some a_1, a_2 and b such that $a_1 p_{x,i} + a_2 p_{y,i} = b$. When we have more than one aircraft, the unsafe set is define as the set where the distance between two aircraft is less than 1 unit distance.

We apply the framework in conflict detection in the following scenario illustrated by Figure 3. In this scenario we have two aircraft, whose flight paths contain a common waypoint. We want to assess the conflict probability of this scenario in the time interval $[0, 1]$. Notice that each realization has two transitions, corresponding to the event when Aircraft-1 switches to Waypoint B and Aircraft-2 switches to Waypoint C.

With Algorithm 1, we can compute that the stochastic hybrid system with the initial condition as shown in Figure 3 is safe in the time interval $[0, 1]$ with probability at least 80%. Moreover, the same probabilistic safety guarantee still

[2]The paper [25] extended the model in [12] into a 3D model. While our framework can adopt the 3D model without significant increase in computation complexity, we choose to adopt the 2D model for simplicity.

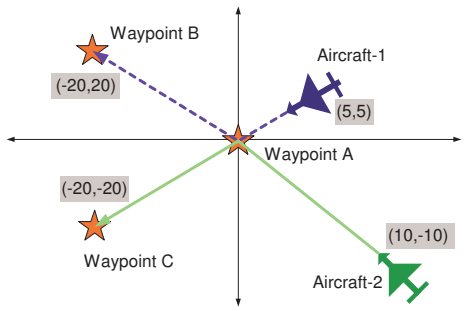

Fig. 3. Flight scenario with two aircraft. Aircraft-1 flies toward Waypoint A and then proceeds to Waypoint B. Aircraft-2 flies toward Waypoint A and proceeds to Waypoint C. The numbers indicate the coordinates of the waypoints and the initial positions of the aircraft.

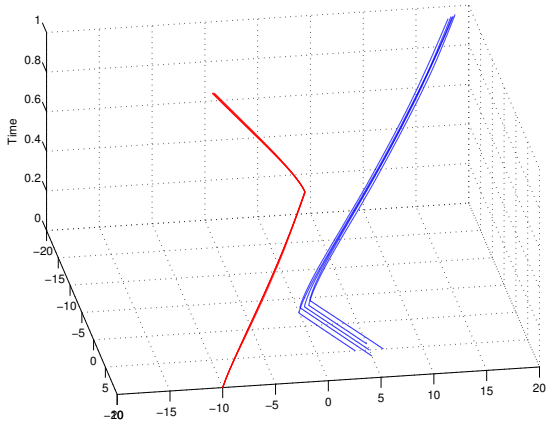

Fig. 4. Several trajectories of Aircraft-1 (right) and Aircraft-2 (left). The vertical axis represents time, the two horizontal axises represent the positions of the aircraft. Each trajectory has two transitions, namely when Aircraft-1 switches to Waypoint B and when Aircraft-2 switches to Waypoint C. We simulate several realization of the trajectory of Aircraft-1 by varying the initial condition.

holds, even if the initial position of Aircraft-1 (or Aircraft-2) is changed from (x_0, y_0) to $(x_0 + \Delta x, y_0 + \Delta y)$ provided that

$$1.44 \cdot \Delta x^2 + \Delta y^2 \leq 1.7821. \tag{33}$$

Several trajectories with the initial position of Aircraft-1 perturbed according to (33) are shown in Figure 4.

V. Concluding Remarks

In this paper we propose a testing based method for safety/reachability analysis of stochastic hybrid systems. The method that we proposed is based on our earlier work on robust testing of deterministic hybrid systems [1]. The main feature of the framework is that safety/reachability is analyzed by evaluating deterministic trajectories of the hybrid nominal system, which is obtained by removing the diffusion part of the original system. We also show that there is a natural trade-off between coverage of the testing and the confidence level of the guarantee provided by the framework.

Acknowledgements. The authors would like to thank Insup Lee, Georgios Fainekos, and Madhukar Anand for valuable discussions in testing and verification.

References

[1] A. A. Julius, G. Fainekos, M. Anand, I. Lee, and G. J. Pappas, "Robust test generation and coverage for hybrid systems," in *Hybrid Systems: Computation and Control*, vol. 4416 of *LNCS*, pp. 329–342, Springer Verlag, 2007.

[2] A. Girard and G. J. Pappas, "Verification using simulation," in *Hybrid Systems: Computation and Control*, vol. 3927 of *LNCS*, pp. 272–286, Springer Verlag, 2006.

[3] M. S. Branicky, M. M. Curtiss, J. Levine, and S. Morgan, "RRTs for nonlinear, discrete, and hybrid planning and control," in *Proc. IEEE Conf. Decision and Control*, (Hawaii, USA), 2003.

[4] J. Kapinski, B. H. Krogh, O. Maler, and O. Stursberg, "On systematic simulation of open continuous systems.," in *Hybrid Systems: Computation and Control*, vol. 2623 of *LNCS*, pp. 283–297, Springer, 2003.

[5] A. Bhatia and E. Frazzoli, "Incremental search methods for reachability analysis of continuous and hybrid systems," in *Hybrid Systems: Computation and Control*, vol. 2993 of *LNCS*, pp. 142–156, Springer Verlag, 2004.

[6] J. Kim, J. M. Esposito, and V. Kumar, "An rrt-based algorithm for testing and validating multi-robot controllers," in *Robotics: Science and Systems*, (Boston, USA), pp. 249–256, 2005.

[7] S. M. LaValle, *Planning algorithms*. Cambridge University Press, 2006.

[8] P. Cheng and V. Kumar, "Sampling-based falsification and verification of controllers for continuous dynamic systems," in *Workshop on Algorithmic Foundations of Robotics VII* (S. Akella, N. Amato, W. Huang, and B. Misha, eds.), 2006.

[9] E. Plaku, L. E. Kavraki, and M. Y. Vardi, "Hybrid systems: From verification to falsification," in *International Conference on Computer Aided Verification*, vol. 4590 of *LNCS*, pp. 468–481, Springer, 2007.

[10] T. Nahhal and T. Dang, "Guided randomized simulation," in *Hybrid Systems: Computation and Control*, vol. 4416 of *LNCS*, pp. 731–735, Springer Verlag, 2007.

[11] J. P. Hespanha, "Polynomial stochastic hybrid systems," in *HSCC* (M. Morari and L. Thiele, eds.), vol. 3414 of *Lecture Notes in Computer Science*, pp. 322–338, Springer Verlag, 2005.

[12] M. Prandini, J. Hu, J. Lygeros, and S. Sastry, "A probabilistic approach to aircraft conflict detection," *IEEE Trans. on Intelligent Transportation Systems*, vol. 1(4), pp. 199–220, 2000.

[13] A. Abate, S. Amin, M. Prandini, J. Lygeros, and S. Sastry, "Computational approaches to reachability analysis of stochastic hybrid systems," in *Hybrid Systems: Computation and Control*, vol. 4416 of *LNCS*, pp. 4–17, Springer Verlag, 2007.

[14] S. Prajna, A. Jadbabaie, and G. J. Pappas, "Stochastic safety verification using barrier certificates," in *Proc. 43rd IEEE Conference on Decision and Control*, (Bahamas), IEEE, 2004.

[15] F. C. Klebaner, *Introduction to stochastic calculus with applications*. London, UK: Imperial College Press, 2005.

[16] A. A. Julius, A. Girard, and G. J. Pappas, "Approximate bisimulation for a class of stochastic hybrid systems," in *Proc. American Control Conference*, (Minneapolis, USA), 2006.

[17] A. A. Julius and G. J. Pappas, "Approximate abstraction of stochastic hybrid systems." provisionally accepted to the IEEE Trans. Automatic Control, 2006.

[18] H. J. Kushner, *Stochastic stability and control*. Mathematics in Science and Engineering: Academic Press, 1967.

[19] A. Girard and G. J. Pappas, "Approximate bisimulations for nonlinear dynamical systems," in *Proc. of the IEEE Conf. Decision and Control*, (Seville, Spain), 2005.

[20] A. Girard and G. J. Pappas, "Approximation metrics for discrete and continuous systems," *IEEE Trans. Automatic Control*, vol. 52, no. 5, pp. 782–798, 2007.

[21] R. Alur, C. Courcoubetis, N. Halbwachs, T. A. Henzinger, P. H. Ho, X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine, "The algorithmic analysis of hybrid systems," *Theoretical Computer Science*, vol. 138, pp. 3–34, 1995.

[22] W. L. Brogan, *Modern control theory*. New Jersey: Prentice Hall International, 1991.

[23] J. Löfberg, "YALMIP: a toolbox for modeling and optimization in MATLAB," in *Proc. CACSD Conference*, 2004.

[24] S. Boyd and M. C. Grant, "cvx – MATLAB software for disciplined convex programming," 2005. http://www.stanford.edu/∼boyd/cvx/.

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