2014 American Control Conference (ACC)
June 4-6, 2014. Portland, Oregon, USA

Combining Analytical Technique and Randomized Algorithm in Safety Verification of Stochastic Hybrid Systems

A. Agung Julius and Alessandro D'Innocenzo

***Abstract*— We consider the problem of probabilistic safety verification for stochastic hybrid systems. In particular, we propose a method that combines two existing approaches, namely, analytical techniques and randomized algorithms. Analytical techniques, such as using stochastic approximate bisimulation, are able to handle non-deterministic initial states. However, their practical applicability is limited to relatively simple stochastic dynamics. On the other hand, randomized algorithms are able to handle more complex dynamics. However, it typically requires running a large number of simulations, and cannot be used for non-deterministic initial states.**

Our combined approach basically uses an analytical technique when the stochastic dynamics is simple, and switches to a randomized algorithm when the dynamics is nonlinear. The main idea is that by using the analytical technique, we can bound the gaps between the probability density functions corresponding to the family of non-deterministic initial states. This, in turn, enables randomized algorithms that provide upper- and lower-bounds on the safety and unsafety probabilities. We illustrate our approach with an example from air traffic management.

Keywords: hybrid systems, verification, randomized algorithms.

I. Introduction

We discuss the notion of *probabilistic safety* for stochastic (hybrid) systems. That is, assessing the probability that a system's execution trajectory enters an unsafe set. In this paper, we distinguish between two types of initiation of stochastic hybrid systems, as illustrated in Figure 1. The first type is systems without non-determinism (Figure 1(a)). In this case, the initial state of the system is assumed to be distributed according to some probability distribution of the state-space. To simulate execution trajectories of this system, a random initial state is drawn from this distribution. Then, the dynamics of the state is described by a continuous time stochastic process, which can involve a combination of ordinary differential equations, stochastic differential equations, and stochastic point processes (see e.g. the review in [1]). The other type of stochastic hybrid systems is those with non-determinism. In this case, the initial state can assume any value in an Init set (see Figure 1(b)). Since the dynamics of the system is still stochastic, we still use the notion of probabilistic safety. However, in the safety verification task, we want to verify that the probabilistic safety property holds for any possible initial state.

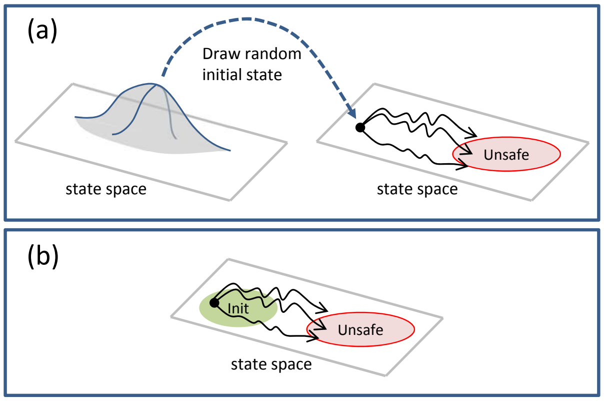

Fig. 1: Illustration for probabilistic safety verification for stochastic (hybrid) systems. (a) System without non-determinism. The initial state is assumed to have a probabilistic distribution. (b) System with non-determinism. The initial state is not random but can assume any value in Init.

A lot of effort has been devoted to safety verification of stochastic hybrid systems. In [2] a procedure has been proposed to derive a finite Markov Chain abstraction with guaranteed approximation error of a discrete-time stochastic hybrid system, while in [3] the notion of approximate probabilistic bisimulation has been used to relate the above approximation error with a notion of robustness for probabilistic model checking (and therefore for safety verification). In [4] probabilistic hybrid systems are considered and a general abstraction technique (based on tools for the analysis of non-probabilistic hybrid systems) for verifying probabilistic safety problems developed. In [5] stochastic continuous-time hybrid systems characterized by non-determinism are considered, and an abstraction and evaluation method is proposed that establishes safe upper bounds on reachability probabilities. In [6] a discrete abstraction of a stochastic discrete-time system describing human motion has been used to estimate the probability of an accident in working environments where human operators and robotic manipulators co-operate. In [7] the authors address the problem of verifying in stochastic hybrid systems temporal logic properties whose probability of being true is very small (rare-events) using a cross-entropy method, since it is well known that Monte Carlo techniques do not perform well for estimating rare-event probabilities. In [8] existing sequential Monte Carlo simulation approaches to estimate rare event probability have been extended towards rarely switching diffusions. In [9] a novel particle filter for a discrete-time stochastic hybrid

Agung Julius is with the Department of Electrical, Computer, and Systems Engineering, Rensselaer Polytechnic Institute, Troy, NY 12180, Email: agung@ecse.rpi.edu. Alessandro D'Innocenzo is with is with the Center of Excellence DEWS, Department of Information Engineering, Computer Science and Mathematics, University of L'Aquila, Italy. Email: alessandro.dinnocenzo@univaq.it

978-1-4799-3274-0/$31.00 ©2014 AACC

system, referred to as the interacting multiple model (IMM) particle filter, is developed.

Because safety verification of stochastic hybrid systems typically involves heavy computation, especially for complex systems, there have also been effort in formalizing abstraction of stochastic hybrid systems. In particular, researchers have looked into ways to create approximate abstraction of stochastic hybrid systems. There are roughly two types of methods for this purpose. The first type relies on analytical results to bound the accuracy of the approximation (see e.g. [10], [11], [12]). The second type relies on randomized algorithm to establish a probabilistic bound of the accuracy of the approximation (see e.g. [13]). There are advantages (and disadvantages) associated to each approach. The advantages of the analytical approach are (i) when possible, it offers a direct answer (e.g. "*the second order moment of the error between the trajectories of the concrete model and the abstract model is less than x*") (ii) it does not involve a large number of simulations, and (iii) it can be used for systems with non-determinism (see e.g. [14]). However, the analytical approach is typically only applicable to a narrow class of systems. For example, stochastic differential equations with linear drift [12]. The advantages of the randomized algorithm approach are (i) it is relatively simple to implement, and (ii) it applies to a wider class of systems since it is simulation based. The disadvantage of using the randomized approach are (i) it can only provide probabilistic answer (e.g. "*the second order moment of the error between the trajectories of the concrete model and the abstract model is less than x with probability at least p*"), (ii) it typically requires a large number of simulations to get statistically significant answer, and (iii) it does not support non-determinism.

The main idea, and the contribution of this paper can be explained as follows. We seek to combine the strengths of the two approaches above. We consider stochastic hybrid sytems where the continuous dynamics is described as stochastic differential equations (SDE) [15] with non-determinism in the initial conditions. Since the continuous dynamics vary with the location/discrete state, in some locations we might be able to use the analytical approach for safety verification, while in other locations we have to resort to randomized algorithms. We develop a framework for combining the results of the two approaches.

II. Problem Formulation

In this preliminary study, for simplicity, we assume that:

A1. The stochastic hybrid system only has two locations. One location, where the initial state can be, has linear continuous dynamics that makes it amenable to analytical technique. The other location, where the Unsafe set is defined, has nonlinear dynamics that requires the use of randomized algorithm.

A2. The transition between one location to another is time-triggered.

Later, we discuss ways to generalize these assumptions. A mathematical description of the problem is as follows.We consider a switched stochastic system with time-triggered switching:

$$dX_{t,x_0} = \begin{cases} (AX_t + b)dt + DdW_t, & 0 \leq t \leq t_s, \\ F(X_t)dt + G(X_t)dW_t, & t > t_s, \end{cases} \qquad (1)$$

with initial state $X_{0,x_0} = x_0$, where $X_{t,x_0} \in \mathbb{R}^n$, W_t is an $m-$dimensional standard Brownian motion, and A, b and D are constant matrices with appropriate dimensions. We assume that the system is non-deterministically initialized in a compact initial set $x_0 \in \mathrm{Init} \subset \mathbb{R}^n$. We also assume that a set of unsafe states, $\mathrm{Unsafe} \subset \mathbb{R}^n$, is given.

To guarantee the existence and uniqueness of the solution of (1), we assume that (c.f. [15]):

A3. F and G are locally Lipschitz: For any $R \in \mathbb{R}_+$, there exists a $K(R) \in \mathbb{R}_+$ such that

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

A4. F and G satisfy linear growth condition: There exists a K' such that for all $x \in \mathbb{R}^n$,

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

Problem 1 (Probabilistic Safety Verification (PSV)): Given the system (1), $\eta > 0$ and $T > t_s$, verify whether for any initial state x_0 ∈Init, the resulting state trajectory X_{t,x_0} remains safe for $t \in (t_s, T]$ with probability larger than $1 - \eta$.

Observe that the safety property that we want to verify in PSV is a mixed of worst-case (for any initial condition) and probabilistic (it should hold with probability larger than $1 - \varepsilon$). The first part of the stochastic dynamics in (1) is assumed to be linear affine. This type of dynamics is known as Ornstein-Uhlenbeck process [15]. Because of its simplicity, many analytical results are known about this process, including the evolution of its probability density, and characterization of its approximate bisimulation function as quadratic functions [16], [12]. The second part is assumed to be a well-posed but nonlinear dynamics, for which analysis we will apply a randomized algorithm.

III. Technical Approach

In principle, this verification task can be completed using the probabilistic testing framework, as reported in [14]. However, this approach requires the computation of stochastic bisimulation functions for both of the dynamics in (1). Assuming that the dynamics after $t = t_s$ is some general nonlinear dynamics, computing a stochastic bisimulation function might not always be possible. Our idea is to exploit a randomized algorithm (see e.g. [17]) to deal with this dynamics.

A. Review of Randomized Algorithms for Probabilistic Safety Verification

Consider a probability space $\mathcal{P} = \{\Omega, \mathcal{F}, \Pr\}$, where Ω is the sample space, $\mathcal{F}$ is the set of events, and $\Pr$ is the probability measure. For any event $e \in \mathcal{F}$, the probability measure $\Pr(e)$ can be estimated by independent samples of Bernoulli trials involving this event. First, we define the indicator function $\mathbf{1}_e : \Omega \to \{0,1\}$ as

$$\mathbf{1}_e(\omega) \triangleq \begin{cases} 1, & \omega \in e, \\ 0, & \omega \notin e. \end{cases}$$

Then, we can draw N independent samples from Ω and denote them as $\{\omega_i\}_{i=1,\cdots,N}$.To these samples, we can associate N independent and identically distributed (i.i.d) binary random variables $\{s_i\}_{i=1,\cdots,N}$, where

$$s_i \triangleq \mathbf{1}_e(\omega_i).$$

Clearly, by definition above

$$\Pr(e) = E[s_i],\ i = 1, \cdots, N. \tag{2}$$

It is well known, and relatively easy to show that

$$\hat{p} \triangleq \frac{1}{N}\sum_{i=1}^{N} s_i \tag{3}$$

is an unbiased estimator of $\Pr(e)$ (see e.g. [18]). The variance of the estimation error is given by

$$E\left[(\Pr(e) - \hat{p})^2\right] = \frac{1}{N}\left(\Pr(e) - \Pr(e)^2\right). \tag{4}$$

To assess the accuracy of the estimator $\hat{p}$, we can use results such as the Chebyshev inequality[18].

$$\Pr\{|\Pr(e) - \hat{p}| \geq \alpha\} \leq \frac{\left(\Pr(e) - \Pr(e)^2\right)}{N\alpha^2} \tag{5}$$

$$\leq \frac{1}{4N\alpha^2}. \tag{6}$$

Consider a stochastic process X_{t,x_0}, $t \in [0,T]$ with fixed initial state at $x_0 \in \mathbb{R}^n$. We can associate this process with a probability space $\mathcal{P}_{x_0} = (\Omega_{x_0}, \mathcal{F}_{x_0}, \Pr_{x_0})$, where Ω_{x_0} contains all realizations of the process. For probabilistic safety verification of this process, we define an event Safe_{x_0} as "the trajectory X_{t,x_0} does not enter the Unsafe set in $[0,T]$". We assume that the Unsafe set and the process are defined in such ways that Safe_{x_0} is measurable. The object of probabilistic safety verification of this process is to assess $\Pr_{x_0}(\mathrm{Safe}_{x_0})$, which can be done following the idea above. In this case, the independent samples of Bernoulli trials are N independent simulations of X_{t,x_0} for $t \in [0,T]$.

In case the initial state is random, i.e. x_0 is randomly distributed on a set Init with $f_X(\cdot) : \mathrm{Init} \to \mathbb{R}$ as the probability density function, the same idea can be applied. In this case, we define a probability space $\mathcal{P} = \{\Omega, \mathcal{F}, \Pr\}$ where the sample space Ω consists of pairs $(x_0, \hat{X}_t)$, with $x_0 \in \mathrm{Init}$ and $\hat{X}_t$ is a realization of the stochastic process starting at $\hat{X}_0 = x_0$. The Safe event is "the state trajectory X_t starting from random initial state X_0 does not enter the Unsafe set in $[0,T]$", which can be characterized as

$$\mathrm{Safe} = \bigcup_{x_0 \in \mathrm{Init}} \{x_0\} \times \mathrm{Safe}_{x_0}. \tag{7}$$

Again, we assume that Safe is measureable. The safety probability $\Pr(\mathrm{Safe})$ can be characterized as

$$\Pr(\mathrm{Safe}) = E\left[\mathbf{1}_{\mathrm{Safe}}\right], \tag{8}$$

where $\mathbf{1}_{\mathrm{Safe}} : \Omega \to \{0,1\}$ is the Safe indicator function. That is,

$$\mathbf{1}_{\mathrm{Safe}}(\omega) \triangleq \begin{cases} 1, & \omega \in \mathrm{Safe}, \\ 0, & \omega \notin \mathrm{Safe}. \end{cases} \tag{9}$$

Using the laws of conditional expectation, we can rewrite (8) as

$$\Pr(\mathrm{Safe}) = E\left[E\left[\mathbf{1}_{\mathrm{Safe}}|x_0\right]\right] = E\left[\Pr_{x_0}(\mathrm{Safe}_{x_0})\right], \tag{10}$$

$$= \int_{\mathrm{Init}} \Pr_{x}(\mathrm{Safe}_x) f_X(x)\ dx. \tag{11}$$

Now, if we define y_0 to be another random variable with probability density function $f_Y(\cdot)$ in $\mathbb{R}^n$, we can interpret (11) as

$$\Pr(\mathrm{Safe}) = \int_{\mathrm{Init}} \Pr_{y}(\mathrm{Safe}_y) f_X(y) \frac{f_Y(y)}{f_Y(y)}\ dy, \tag{12}$$

$$= \int_{\mathrm{Init}} \Pr_{y}(\mathrm{Safe}_y) \frac{f_X(y)}{f_Y(y)} \cdot f_Y(y)\ dy. \tag{13}$$

From (13), we can define a randomized algorithm to estimate Pr(Safe), as shown in Algorithm 1. Here, we can see that (13) provides us with an alternative formulation of (11) in case that the random initial state samples are drawn from a different (but known) distribution from the actual distribution of the initial state.

Algorithm 1 Randomized algorithm to estimate $\Pr(\mathrm{Unsafe})$ using N samples.

```
Require: An Init set with finite nonzero Lebesque measure
    and a probability density function $f_X(\cdot)$ on Init for the
    initial state, and a probability density function $f_Y(\cdot)$ on
    Init for the samples,
for all $i \in \{1, \ldots, N\}$ do
    Draw a random initial state $y_i$ from the probability
      density function $f_Y(\cdot)$ on Init.
    Draw $\hat{X}_t^i$, which is a realization of the stochastic
      process $X_t$ starting at $\hat{X}_0^i = y_i$.
    Define a variable $s_i$, where $s_i = \frac{f_X(y_i)}{f_Y(y_i)}$ if $\hat{X}_t^i$ is safe,
      and $s_i = 0$ otherwise.
end for
An unbiased estimator of Pr(Safe) is given by
    $\hat{p} \triangleq \frac{1}{N}\sum_{i=1}^{N} s_i.$    (14)
```

The use of randomized algorithms in lieu of analytical techniques, such as approximate bisimulation [16], [12], for computing approximate abstraction of stochastic systems has been previously done in [13]. However, plain randomized algorithms are not applicable in PSV. This is because the system contains non-determinism in the initial condition, while randomized algorithms cannot handle non-determinism. One approach is to assume that Init is endowed with an arbitrary probability measure, e.g. uniform distribution [19]. However, it is clear that this does not address the PSV problem.

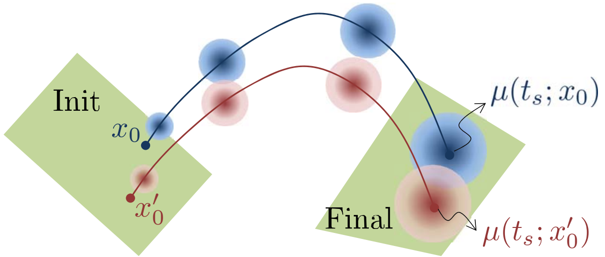

Fig. 2: An illustration how the mean and covariance of the Ornstein-Uhlenbeck process changes with initial condition.

B. *Combining Analytical and Randomized Algorithms*

We propose a novel method that combines an analytical method with a randomized algorithm to solve PSV.

1) Calculating the Mean and Covariance of the Ornstein-Uhlenbeck Process: First, we focus on the dynamics of the system in (1) for $t \in [0, t_s]$. This is an Ornstein Uhlenbeck process [15]. The probability density function of X_{t,x_0} for a given initial condition $x_0 \in \text{Init}$ and $t \in [0, t_s]$, $p(x,t;x_0)$, can be expressed as:

$$p(x,t;x_0) = \mathcal{N}(x;\mu(t;x_0),\Phi(t)), \tag{15}$$

where $\mathcal{N}(\cdot;\mu,\Phi)$ is the normal probability density function with mean vector μ and covariance matrix Φ. The mean of $p(x,t)$ is given by

$$\mu(t;x_0) = e^{At}x_0 + \int_0^t e^{A(t-\tau)}b\;d\tau. \tag{16}$$

The covariance matrix $\Phi(t;x_0)$ satisfies the ODE

$$\frac{d\Phi(t)}{dt} = A\Phi(t) + \Phi(t)A^T + DD^T, \tag{17}$$

$$\Phi(0) = 0. \tag{18}$$

2) Bounding the Impact of Initial State Variation: If we vary the initial state from x_0 to x_0', (17) indicates that the covariance matrix will not be affected. The mean trajectory will evolve as (see Figure 2)

$$\mu(t;x_0') - \mu(t;x_0) = e^{At}\left(x_0' - x_0\right). \tag{19}$$

We define the final set

$$\text{Final} \triangleq \{x \mid \exists x_0 \in \text{Init s.t. } \mu(t_s;x_0) = x\}. \tag{20}$$

Notation 1: We introduce the following shorthand notations for the subsequent discussion.

$$\|x\|_\Phi \triangleq \sqrt{x^T\Phi^{-1}(t_s)x}, \tag{21}$$

$$B_\Phi(x_0,r) \triangleq \{x \in \mathbb{R}^n \mid \|x - x_0\|_\Phi \leq r\}. \tag{22}$$

Next, we define the radius of the Final set as

$$r_{\max} = \min\{r > 0 \mid \exists x \in \mathbb{R}^n \text{ s.t. Final} \subset B_\Phi(x,r)\}, \tag{23}$$

and its center x_c as

$$\text{Final} \subset B_\Phi(x_c, r_{\max}). \tag{24}$$

In the following, we shall bound the difference between the density functions $p(x,t_s;x_0)$ and $\mathcal{N}(x;x_c,\Phi(t_s))$, for any x_0 in Init.

Theorem 1: For any $x \in \mathbb{R}^n$,

$$\max_{x_0\in\text{Init}} \frac{p(x,t_s;x_0)}{\mathcal{N}(x;x_c,\Phi(t_s))} = \exp\left(\frac{\|x-x_c\|_\Phi^2 - f_*(x)}{2}\right), \tag{25}$$

$$\min_{x_0\in\text{Init}} \frac{p(x,t_s;x_0)}{\mathcal{N}(x;x_c,\Phi(t_s))} = \exp\left(\frac{\|x-x_c\|_\Phi^2 - f^*(x)}{2}\right), \tag{26}$$

where

$$f_*(x) \triangleq \min_{y\in\text{Final}} \|x-y\|_\Phi^2, \tag{27}$$

$$f^*(x) \triangleq \max_{y\in\text{Final}} \|x-y\|_\Phi^2. \tag{28}$$

Proof: By definition,

$$\max_{x_0\in\text{Init}} \frac{p(x,t_s;x_0)}{\mathcal{N}(x;x_c,\Phi(t_s))} = \max_{y\in\text{Final}} \frac{\mathcal{N}(x;y,\Phi(t_s))}{\mathcal{N}(x;x_c,\Phi(t_s))},$$

$$= \max_{y\in\text{Final}} \exp\left(\frac{\|x-x_c\|_\Phi^2 - \|x-y\|_\Phi^2}{2}\right). \tag{29}$$

We can prove (26) in a similar way. ■

Remark 2: The calculation of $f_*(x)$ and $f^*(x)$ involves maximization or minimization of a quadratic cost over a general set, which might be non-convex optimization. However, if Init is a polytope (and so is Final), these optimization problems have linear constraints, which can be solved reliably [20]. In particular, both $f_*(x)$ and $f^*(x)$ are piecewise quadratic functions.

3) Proposed Algorithm: We can adapt Algorithm 1 to solve the probabilistic safety verification by computing a lower bound for the safety probability and an upper bound for the unsafety probability as shown in Algorithm 2.

Theorem 3: Consider $p_*(\text{Safe})$ and $p^*(\text{Unsafe})$ obtained from Algorithm 2. For any $x_0 \in \text{Init}$ and $\alpha > 0$, the probability that the state trajectory X_{t,x_0} remains safe for $t \in (t_s, T]$ is larger than $(p_*(\text{Safe}) - \alpha)$ with probability larger than $\left(1 - \frac{1}{4N\alpha^2}\right)$. Also, the probability that the state trajectory X_{t,x_0} is unsafe is larger than $(p^*(\text{Unsafe}) + \alpha)$ with probability larger than $\left(1 - \frac{1}{4N\alpha^2}\right)$.

Proof: The first part can be proved as follows. For any $x_0 \in \text{Init}$, let us define $p_{x_0}(\text{Safe})$ as the output of Algorithm 2 if we replaced (30) with

$$l_i = \frac{p(y_i,t_s;x_0)}{\mathcal{N}(y_i;x_c,\Phi(t_s))}. \tag{34}$$

Following Algorithm 1, we note that $p_{x_0}(\text{Safe})$ is an unbiased estimation of the safety probability of X_{t,x_0}. Further, from (6) we can infer that the safety probability of X_{t,x_0} is larger than $(p_{x_0}(\text{Safe}) - \alpha)$ with probability larger than $\left(1 - \frac{1}{4N\alpha^2}\right)$. Combining this with (26), we can infer that $p_{x_0}(\text{Safe})$ is lower bounded by $p_*(\text{Safe})$. The second part of the theorem can be proved similarly. ■

Algorithm 2 Computation of a lower bound of the safety probability with N random samples

```
Require: A Final set, and a probability density function $\mathcal{N}(x; x_c, \Phi(t_s))$ for the samples,
for all $i \in \{1, \dots, N\}$ do
    Draw a random initial state $y_i$ from the probability density function $\mathcal{N}(x; x_c, \Phi(t_s))$.
    Draw $\hat{X}_t^i$, which is a realization of the stochastic process $X_t$ for $t \in (t_s, T]$ starting at $\hat{X}_{t_s}^i = y_i$.
    Define a variable $l_i$, where
        $l_i = \exp\left(\frac{\|y_i - x_c\|_\Phi^2 - f^*(y_i)}{2}\right)$    (30)
    if $\hat{X}_t^i$ is safe, and $l_i = 0$ otherwise.
    Define a variable $u_i$, where
        $u_i = \exp\left(\frac{\|y_i - x_c\|_\Phi^2 - f_*(y_i)}{2}\right)$    (31)
    if $\hat{X}_t^i$ is unsafe, and $u_i = 0$ otherwise.
end for
A lower bound of $\Pr(\text{Safe})$ is given by
    $p_*(\text{Safe}) \triangleq \frac{1}{N}\sum_{i=1}^{N} l_i.$    (32)
An upper bound of unsafety probability $\Pr(\text{Safe}^c)$ is given by
    $p^*(\text{Unsafe}) \triangleq \frac{1}{N}\sum_{i=1}^{N} u_i.$    (33)
```

Note that, although it might be intuitive to expect that because the probabilities of safety and unsafety add up to 1,

$$E\left[p^*(\text{Unsafe})\right] + E\left[p_*(\text{Safe})\right] = 1. \tag{35}$$

This is generally not the case. This is true, however, if $r_{\max} = 0$, which would imply

$$\|x - x_c\|_\Phi^2 = f_*(x) = f^*(x).$$

IV. Example

We present a realistic case study in air traffic management. Assume that an aircraft, starting from a non-deterministic initial position within a compact set, navigates at constant cruising speed, altitude and heading angle. During the straight cruise phase the aircraft behavior is quite robust with respect to disturbances and can be appropriately modeled using a Brownian Motion where the drift is given by affine dynamics. After a predefined time t_1, the aircraft performs a veer because of its flight plan. During the veer the aircraft behavior is quite more complex and can be appropriately modeled using a Brownian Motion where the drift is given by nonlinear dynamics.

Given an unsafe area where the system is not allowed to fly (see [21] for details), we wish to compute the worst case probability (for any initial condition) that the aircraft will enter the unsafe area within a given time horizon $t_2 > t_1$. Because of the mixed stochastic and non-deterministic structure of the model and for the reasons discussed above classical techniques are not applicable, thus we will use the new procedure developed in this paper.

We use a point mass model for the aircraft dynamics and assume that the altitude is constant and equal to flight level 350 (35000 feet). When the aircraft is performing a veer we adopt from [22] and [21] the following Brownian Motion model where the drift is given by nonlinear dynamics:

$$\begin{aligned}
dX &= V\cos(\psi)\cos(\gamma)dt + d_1 dw_1\\
dY &= V\sin(\psi)\cos(\gamma)dt + d_2 dw_2\\
\dot{V} &= -k_1\frac{V^2}{m} - g\sin(\gamma) + \frac{T}{m}\\
\dot{\psi} &= k_2\frac{V}{m}\sin(\phi)\\
\dot{m} &= -\mu T.
\end{aligned}$$

The state space $x \in \mathbb{R}^5$ consists of X, Y the horizontal position, V the true airspeed, ψ the yaw angle and m the aircraft mass. The input space consists of T the engine thrust, ϕ the roll angle and γ the pitch angle. During the veer we will assume that the inputs are constant: $T = 3000\ Kg\ m/s^2$, $\phi = 0.1\ rad$ ($5.7\ deg$) and $\gamma = 0\ rad$. g is the gravity acceleration, $k_1 = 1.31\ Kg/m$, $k_2 = 25.545\ Kg/m$, and $\mu = 0.001\ s/m$. Wind is considered as a disturbance on the aircraft dynamics, and is modeled as a Brownian motion with $d_1 = d_2 = 13.9\ m/s$. The values for the above simulation parameters have been taken from the database BADA (Base of Aircraft DAta) [23].

When the aircraft is navigating at constant cruising speed, altitude and heading angle, we adopt the following simplified Brownian Motion model where the drift is given by affine dynamics:

$$\begin{aligned}
dX &= Vdt + d_1 dw_1\\
dY &= -\lambda_2 Y dt + d_2 dw_2\\
\dot{V} &= 0\\
\dot{\psi} &= 0\\
\dot{m} &= -\mu T,
\end{aligned}$$

with $\lambda_2 = 0.01$. During the cruising phase we will assume that the inputs are constant: $T = 3000\ Kg\ m/s^2$, $\phi = 0\ rad$ and $\gamma = 0\ rad$.

We assume that the aircraft initial position belongs non-deterministically to the set $\text{Init} = \{x \in \mathbb{R}^5 : X(0) \in [-500, +500]\ m, Y(0) \in [-500, +500]\ m, V(0) = 237\ m/s, \psi(0) = 0\ rad, m(0) = 150000\ Kg\}$, that the unsafe set is give by $\text{Unsafe} = \{x \in \mathbb{R}^5 : X > 890000\ m \wedge Y < 2000\ m\}$ and that $t_1 = 1h$, $t_2 = 1h5min$. We implemented the procedure described in the above sections on MATLAB and used a polytopic overapproximation of the set Final of Equation (20), which made the computation of $f_*(x)$ in Algorithm 2 easily solvable using quadratic programming. Using just 250000 runs we were able to verify

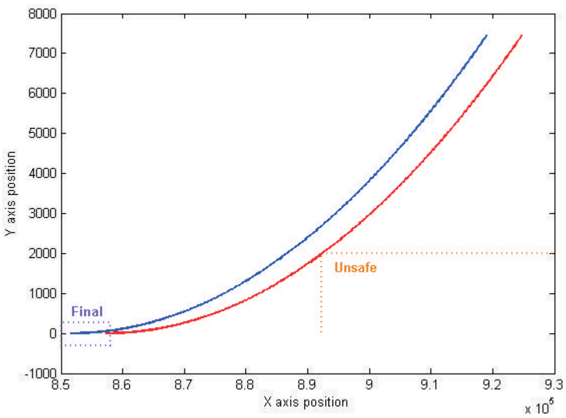

Fig. 3: Two sample trajectories from the set $Final$ for $t \in [t_1, t_2]$, one safe (blue) and one unsafe (red).

the following proposition: *the probability that, for any initial state in* Init*, the trajectories of the aircraft remain safe for* $t \in [0, t_2]$ *is larger than 0.9894 with probability (confidence) larger than 0.01.*

V. Discussion and Future Directions

In this paper we present a method to combine the use of analytical techniques and randomized algorithms in probability safety verification of stochastic hybrid systems. In particular, the analytical technique allows us to deal with the case where the initial states are non-deterministic, and we are interested in the worst case safety probability.

As this is a preliminary work towards this interesting direction, we setup a relatively simple problem, which is bound by the assumptions in Section II. In particular, we assume that the simple dynamics is affine linear and its location does not have Unsafe set. Also, we assume for time triggered transition, as opposed to event/guard triggered transition. These assumptions were made to ensure that we can compute the evolution of the probability density function analytically. If we had defined event/guard triggered transitions or Unsafe set at the first location, then the evolution of the probability density function would satisfy the Fokker-Planck equation with the guard and/or the Unsafe set acting as an absorbing or Dirichlet boundary condition [15]. While the computation of the density functions in this case is not as simple as the one in this paper, it is interesting to explore if we can establish a bound similar to Theorem 1.

Another interesting direction to explore is tightening the bound given by the Chebyshev's inequality in (6) by using other results, such as Chernoff's inequality.

VI. Acknowledgements

The research reported in this paper is partially supported by the NSF through the grant CAREER CNS-0953976.

References

[1] G. Pola, M. Bujorianu, J. Lygeros, and M. D. Benedetto, "Stochastic hybrid models: an overview," in *Proc. IFAC Conf. Analysis and Design of Hybrid Systems*. St. Malo: IFAC, 2003.

[2] A. Abate, A. D'Innocenzo, and M. D. Benedetto, "Approximate abstractions of stochastic hybrid systems," *IEEE Transactions on Automatic Control*, vol. 56, no. 11, pp. 2688–2694, 2011.

[3] A. D'Innocenzo, A. Abate, and J.-P. Katoen, "Robust pctl model checking," in *15th ACM international conference on Hybrid Systems: Computation and Control, ACM New York, NY, USA*, 2012, pp. 275–286.

[4] L. Zhang, Z. She, S. Ratschan, H. Hermanns, and E. M. Hahn, "Safety verification for probabilistic hybrid systems," in *22nd International Conference on Computer Aided Verification (CAV2010), Edinburgh, UK, July 15-19*, ser. Lecture Notes in Computer Science, B. C. T, Touili and P. Jackson, Eds., vol. 6174. Springer Berlin Heidelberg, 2010, pp. 196–211.

[5] M. Fränzle, E. M. Hahn, H. Hermanns, N. Wolovick, and L. Zhang, "Measurability and safety verification for stochastic hybrid systems," in *Proceedings of the 14th international conference on Hybrid systems: computation and control*, ser. HSCC '11. New York, NY, USA: ACM, 2011, pp. 43–52. [Online]. Available: http://doi.acm.org/10.1145/1967701.1967710

[6] R. Asaula, D. Fontanelli, and L. Palopoli, "Safety provisions for human/robot interactions using stochastic discrete abstractions," in *IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS2010)*, 2010, pp. 2175–2180.

[7] P. Zuliani, C. Baier, and E. Clarke, "Rare-event verification for stochastic hybrid systems," in *15th ACM international conference on Hybrid Systems: Computation and Control, ACM New York, NY, USA*, 2012, pp. 217–226.

[8] J. Krystul and H. A. P. Blom, "Sequential Monte Carlo simulation of rare event probability in stochastic hybrid systems," in *Proc. IFAC World Congress*, 2005.

[9] H. Blom and E. Bloem, "Particle filtering for stochastic hybrid systems," in *43rd IEEE Conference on Decision and Control, December 14-17, Atlantis, Paradise Island, Bahamas*, 2004, pp. 3221–3226 (Vol.3).

[10] A. Singh and J. P. Hespanha, "Approximate moment dynamics for chemically reacting systems," *IEEE Trans. Automatic Control*, vol. 56, pp. 414–418, 2011.

[11] B. Munsky and M. Khammash, "The finite state projection algorithm for the solution of the chemical master equation," *J. Chemical Physics*, vol. 124, p. 044104, 2006.

[12] A. A. Julius and G. J. Pappas, "Approximate abstraction of stochastic hybrid systems," *IEEE Trans. Automatic Control*, vol. 54(6), pp. 1193–1203, 2009.

[13] A. Abate and M. Prandini, "Approximate abstractions of stochastic systems: a randomized method," in *Proc. IEEE Conf. Decision and Control*, 2011.

[14] A. A. Julius and G. J. Pappas, "Probabilistic testing for stochastic hybrid systems," in *Proc. IEEE Conf. Decision and Control*, Cancun, Mexico, 2008, pp. 4030–4035.

[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] R. Tempo, G. Calafiore, and F. Dabbene, *Randomized Algorithms for Analysis and Control of Uncertain Systems*. Springer, 2005.

[18] A. Papoulis and S. U. Pillai, *Probability, Random Variables and Stochastic Processes*, 4th ed. McGraw-Hill, 2002.

[19] G. C. Calafiore and M. C. Campi, "The scenario approach to robust control design," *IEEE Trans. Automatic Control*, vol. 51, no. 5, pp. 742–753, 2006.

[20] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004, available online at www.stanford.edu/ boyd/cvxbook/.

[21] M. D. Benedetto, G. D. Matteo, and A. D'Innocenzo, "Stochastic validation of atm procedures by abstraction algorithms," in *4th International Conference on Research in Air Transportation, Budapest, Hungary, June 1-4*, 2010.

[22] W. Glover and J. Lygeros, "Deliverable number d1.3: A multi-aircraft model for conflict detection and resolution algorithm evaluation," HYBRIDGE, Tech. Rep., February 18 2004, project: Distributed Control and Stochastic Analysis of Hybrid Systems Supporting Safety Critical Real-Time Systems Designe.

[23] "www.eurocontrol.int/eec/public/standard_page/proj_bada.html."