Software Engineering Group
Department of Computer Science
Nanjing University
http://seg.nju.edu.cn

Technical Report No. NJU-SEG-2017-IJ-003

2017-IJ-003

Safety Verification of Stochastic Hybrid Systems Using Barrier Certificates

Chao Huang, Xin hen,WangLin, hengfeng Yang, and Xuandong Li

ACM Transactions on Embedded Computing Systems 2017

Probabilistic Safety Verification of Stochastic Hybrid Systems Using Barrier Certificates

CHAO HUANG and XIN CHEN, State Key Lab for Novel Software Technology, Nanjing University
WANG LIN, Key Lab of Mathematics Mechanization, AMSS
ZHENGFENG YANG, East China Normal University
XUANDONG LI, State Key Lab for Novel Software Technology, Nanjing University

The problem of probabilistic safety verification of stochastic hybrid systems is to check whether the probability that a given system will reach an unsafe region from certain initial states can be bounded by some given probability threshold. The paper considers stochastic hybrid systems where the behavior is governed by polynomial equalities and inequalities, as for usual hybrid systems, but the initial states follow some stochastic distributions. It proposes a new barrier certificate based method for probabilistic safety verification which guarantees the absolute safety in a infinite time horizon that is beyond the reach of existing techniques using either statistical model checking or probabilistic reachable set computation. It also gives a novel computational approach, by building and solving a constrained optimization problem coming from verification conditions of barrier certificates, to compute the lower bound on safety probabilities which can be compared with the given threshold. Experimental evidence is provided demonstrating the applicability of our approach on several benchmarks.

CCS Concepts: • **Theory of computation** → **Timed and hybrid models**; • **Computer systems organization** → **Embedded software**; • **Software and its engineering** → **Formal software verification**; • **Mathematics of computing** → *Probability and statistics*;

Additional Key Words and Phrases: Stochastic hybrid systems, safety verification, barrier certificate

ACM Reference format:
Chao Huang, Xin Chen, Wang Lin, Zhengfeng Yang, and Xuandong Li. 2017. Probabilistic Safety Verification of Stochastic Hybrid Systems Using Barrier Certificates. *ACM Trans. Embed. Comput. Syst.* 16, 5s, Article 186 (September 2017), 19 pages.
https://doi.org/10.1145/3126508

This article was presented in the 2017 International Conference on Embedded Software and appears as part of the ESWEEK-TECS special issue.
This material is supported in part by the National Natural Science Foundation of China under Grants 61632015, 61561146394, 61602348 and 11471209, Shanghai Natural Science Foundation under Grant 17ZR1408300, and the China Scholarship Council under Grant 201606190185. We would like to thank anonymous reviewers for their very valuable comments.
Author's addresses: C. Huang and X. Chen, State Key Lab for Novel Software Technology, Nanjing University, Jiangsu 210023, China; email: {huangchao, chenxin}@nju.edu.cn; W. Lin, Key Lab of Mathematics Mechanization, Academy of Mathematics and Systems Science, CAS, Beijing 100190, China; email: linwang@wzu.edu.cn; Z. Yang (corresponding author), Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, Shanghai 200062, China; email: zfyang@sei.ecnu.edu.cn; X. Li, State Key Lab for Novel Software Technology, Nanjing University, Jiangsu 210023, China; email: lxd@nju.edu.cn.

https://doi.org/10.1145/3126508

1 INTRODUCTION

Stochastic hybrid systems are dynamical systems involving interacting discrete, continuous and stochastic dynamics [25]. They arise naturally when modelling embedded systems consisting of components with uncertainty, exhibiting random behaviors or running in an environment governed by dynamics with probabilistic parameters. They are widely used in the design and verification of practical embedded systems, such as air traffic management systems [13], networked control systems [16], communication networks [15], and autonomous vehicles [2].

The problem of probabilistic safety verification of stochastic hybrid systems is to compute the probability of reaching a certain set of dangerous states when they are starting from an initial set. It helps to verify the safety issues of systems, especially those safety-critical systems, for whom assuring they will never enter any dangerous state in an infinite time horizon is a primary requirement. It is an arduous and challenging problem which is undecidable in general [36].

There are several types of stochastic hybrid systems [14, 18, 35] which are different on which stochastic characteristics are integrated in. In this paper, we focus on the probabilistic safety verification of the class of semi-algebraic stochastic hybrid systems where the dynamics are represented as polynomial relations (equalities and inequalities) over the system variables and random variables appearing in the initial mode satisfy a specified probability distribution. Such a class of stochastic hybrid systems is a prerequisite for quantitative analysis of nonlinear embedded systems starting with random initial states as a result of running in a randomly behaved environment whose state space is characterized by random distribution functions.

Most of existing works use either statistical model checking [23, 24] or probabilistic reachable set computation [32, 33] to verify stochastic hybrid systems. However, rather than offering the absolute guarantees, statistical model checking can only provide statistical guarantees [11]. Reachable set computation based techniques can give absolutely correct results complying with the classic semantics of verification [10, 31], but is restricted to a finite number of discrete steps. Neither of them can fully satisfy the requirement of verifying the safety property: being absolutely safe in an infinite time horizon coming from many practical applications, e.g. safety-critical systems.

For conventional hybrid systems, barrier certificate generation based techniques [19, 20, 28, 37] have been well developed for safety verification due to its less computational difficulty than reachable set computation and its ability to tackle infinite time. In the paper, we propose a novel method for probabilistic safety verification of semi-algebraic hybrid systems with stochastic initial states based on barrier certificates.

The key idea is inspired by the observation that if we can mark an initial state region for which there exists a corresponding barrier certificate, it can be concluded that the system is safe starting from the region. Meanwhile, the volume ratio of the region to the initial state space gives a lower bound of safety probability. Following this, in order to enlarge this lower bound, the problem of probabilistic safety verification is transferred to the problem of finding a maximal inscribed region in the initial state space for which a barrier certificate can be found.

In theory, the maximal inscribed region is not computable. Consequently, the relatively maximal inscribed region can be found by exhaustedly testing that enumerates various regions of different shapes with all possible parameters. However, it requires too much computation efforts which is sometimes unbearable and may not provide dependable results within a great number of trials, thus is difficult to adopt in practice.

To make it amenable, we propose a computational method as well as the procedure, called Probabilistic Barrier Certificates Generation (PBCG), for predicting the exact lower bound of the safety probability which begins with designing region templates of different shapes customized to the

stochastic distribution of initial states, and is followed by calculating the area with the highest probability subjecting to the parameterized initial template.

Specifically, our PBCG procedure consists of two steps: First, a constrained optimization problem is built which puts the maximal size of the given region template as the objective function and encodes the verification conditions of probabilistic barrier certificates as constraints. Then, to make the optimization problem amenable, it is further encoded by sum of squares (SOS) relaxation as a SOS program yielding a non-convex bilinear matrix inequalities (BMI) problem, which can be resolved by employing the PENBMI solver [21]. The solution of the problem gives the lower bound of the exact safety probability. Clearly, the safety property can be definitely guaranteed if this lower bound we compute is higher than the target safety property derived from the given threshold of unsafe probability.

The main contributions of this paper are summarized as follows: 1. We propose a new probabilistic barrier certificate based method for safety verification of hybrid systems with stochastic initial states, which gives absolute probability guarantees in an infinite time horizon. 2. Rather than evaluating the maximal safety probability by enumerating all possible settings of region templates, we suggest a new computational approach, by solving a constrained optimization problem yielded from the probabilistic safety probability, to compute the lower bound of the exact safety probability. 3. We provide a detailed experimental evaluation on a set of benchmarks, which shows that the guaranteed probabilities given by our method are closed to the best ones obtained by random testing.

The rest of this paper is organized as follows. We introduce some related notations about stochastic hybrid system in Section 2 and then define probabilistic barrier certificates for probabilistic safety verification in Section 3. We transfer the problem of generating probabilistic barrier certificates to a constrained optimization problem and solve it in Section 4. Evaluations on some benchmarks are shown in Section 5 before concluding in Section 6.

2 STOCHASTIC HYBRID SYSTEMS

A stochastic hybrid system was introduced by [36]. The main difference with the model introduced in [11, 12, 36] is that here we are interested in hybrid systems with stochastic initial states. We slightly modify the formulation in [3], and use the notion of stochastic hybrid automata to model the stochastic hybrid system.

Definition 2.1 (Stochastic Hybrid Automata). A *stochastic hybrid automaton* is a system $\mathbf{SH} : \langle L, X, F, \Psi, E, G, R, \Omega, \ell_0 \rangle$, where

- L, a finite set of locations (or modes);
- $X \subseteq \mathbb{R}^n$ is the continuous state space. The hybrid state space of the system is defined by $\mathcal{X} = L \times X$ and a state is defined by $(\ell, \mathbf{x}) \in \mathcal{X}$;
- $F : L \to (\mathbb{R}^n \to \mathbb{R}^n)$ assigns to each location $\ell \in L$, a locally determined Lipschitz continuous vector field $\mathbf{f}_\ell$

$$\dot{\mathbf{x}} = \mathbf{f}_\ell(\mathbf{x}); \tag{1}$$

- Ψ assigns to each location $\ell \in L$, a *location condition (location invariant)* $\Psi(\ell) \subseteq \mathbb{R}^n$;
- $E \subseteq L \times L$ is a finite set of discrete transitions;
- G assigns to each transition $e \in E$, a switching guard $G_e \subseteq \mathbb{R}^n$;
- R assigns to each transition $e \in E$, a reset function $R_e : \mathbb{R}^n \to \mathbb{R}^n$;
- Ω, the initial distribution, which is used to choose the initial continuous state;
- $\ell_0 \in L$, the initial location.

In this paper, we focus on stochastic hybrid systems whose elements are represented as polynomial relations (equalities and inequalities) over the system variables.

Definition 2.2. [Semi-algebraic Stochastic Hybrid System] A semi-algebraic stochastic hybrid system is a stochastic hybrid system: $\mathbf{SH} : \langle L, X, F, \Psi, E, G, R, \Theta, \ell_0 \rangle$, where

- the continuous vector field $F(\ell)$ for each $\ell \in L$ is of the form $\dot{\mathbf{x}} = \mathbf{f}_\ell(\mathbf{x})$, where $\mathbf{f}_\ell(\mathbf{x}) \in \mathbb{R}[\mathbf{x}]^n$;
- the location invariant $\Psi(\ell)$ for each $\ell \in L$, and the guard condition G_e for each $e \in E$ are semi-algebraic sets defined by polynomial inequalities with variables $\mathbf{x}$; $R_e \in \mathbb{R}[\mathbf{x}]^n$ is the reset function for each $e \in E$.

A trajectory of **SH** is an infinite sequence of states

$$(l_0, \mathbf{x}_0),\ (l_1, \mathbf{x}_1), \ldots, (l_i, \mathbf{x}_i),\ (l_{i+1}, \mathbf{x}_{i+1}), \ldots$$

such that

- **[Initiation]** $(l_0, \mathbf{x}_0) \in \ell_0 \times \Psi(\ell)$.
  Furthermore, for each consecutive pair $(l_i, \mathbf{x}_i), (l_{i+1}, \mathbf{x}_{i+1})$, one of the two *consecution* conditions holds:
- **[Discrete Consecution]** $e = (l_i, l_{i+1}) \in E$, $\mathbf{x}_i \in G_e$ and $x_{i+1} = R_e(\mathbf{x}_i)$; or
- **[Continuous Consecution]** $l_i = l_{i+1} = \ell$, and there exists a time interval $\delta > 0$ such that the solution $\mathbf{x}(\mathbf{x}_i; t)$ to $\dot{\mathbf{x}} = \mathbf{f}_\ell(\mathbf{x})$ evolves from $\mathbf{x}_i$ to $\mathbf{x}_{i+1}$, while satisfying the location invariant $\Psi(\ell)$. Formally,
  $-\mathbf{x}(\mathbf{x}_i, \delta) = \mathbf{x}_{i+1}$ and
  $-\forall t \in [0, \delta], \mathbf{x}(\mathbf{x}_i, t) \in \Psi(\ell)$.

Given a semi-algebraic stochastic hybrid system **SH** with prespecified unsafe state set $\ell \times X_u$, we focus on the following probabilistic safety problem: determine the probability that **SH** will remain within a prespecified "safe" set, starting from random initial variables $\mathbf{x}_0$ satisfying Ω, i.e. the probability that **SH** does not reach the unsafe state set X_u. Before calculating the safety probability, we first define the set $\mathcal{I}$ that contains all the initial states of the random variables, starting from which the trajectories will never reach the unsafe state set. We refer to the set $\mathcal{I}$ as the *safe initial state set*, which can be constructed in the following way.

Definition 2.3 (Safe Initial State Set). Let **SH** be a semi-algebraic stochastic hybrid system with an unsafe region X_u. For each location $\ell \in L$, assume $\mathbf{x}_\ell(x_0, t)$ is the solution to $\dot{\mathbf{x}} = \mathbf{f}_\ell(\mathbf{x})$ where x_0 is the initial state. Let

$$G_\ell(A) = \{y : \exists x_0 \in A, t \geq 0, s.t.\ y = \mathbf{x}_\ell(x, t)\}, \tag{2}$$

For a given trajectory, let C_i be a map determined by the consecution from $(\ell_i, \mathbf{x}_i)$ to $(\ell_{i+1}, \mathbf{x}_{i+1})$:

$$C_i = \begin{cases} R_{(l_i, l_{i+1})}, & \text{if the consecution is discrete,} \\ G_{\ell_i}, & \text{if the consecution is continuous.} \end{cases} \tag{3}$$

Let $\mathfrak{A}_i$ be the set consisting of the initial states where the trajectories will enter the unsafe region X_u within the first i-th consecution, namely,

$$\mathfrak{A}_i = C_0^{-1}(C_1^{-1}(\cdots(C_i^{-1}(X_u) \cap \Psi(l_i)) \cdots) \cap \Psi(l_1)) \cap \Psi(l_0)).$$

Then the safe initial state set $\mathcal{I}$ can be represented as

$$\mathcal{I} = \bigcap_{i=0}^{\infty} \overline{\mathfrak{A}_i} \cap \Psi(l_0).$$

Intuitively, $\mathcal{I}$ above can be interpreted as the subset of $\Psi(\ell_0)$ by removing the unsafe initial states calculated from all the trajectories from the initial local invariant $\Psi(\ell_0)$.

To make probabilities well defined, we need to ensure that the safe initial state set $\mathcal{I}$ is Borel. Note that $\Psi(\ell_l)$ is a semi-algebraic set represented by finite polynomial inequalities. So $\Psi(\ell_l)$ is Borel. The key is to prove that the inverse image of a Borel set under C_i^{-1} is also Borel, which is shown in the following lemma.

Lemma 2.4. *For any $\ell \in L$, if A is a Borel set, then $C_i^{-1}(A)$ is also Borel.*

Theorem 2.5. *The safe initial state set $\mathcal{I}$ is Borel.*

Proof. The desired result can be easily yielded from Lemma 2.4 and Definition 2.3. □

Theorem 2.5 ensures the safety probability of the system is well-defined. We can compute such a probability P by integrating the probability density function $f(\mathbf{x})$ over $\mathcal{I}$ of random variable $\mathbf{x}$:

$$P_{\text{safe}} = \int_{\mathcal{I}} f(\mathbf{x}) d\mathbf{x}. \tag{4}$$

3 BARRIER CERTIFICATES FOR STOCHASTIC HYBRID SYSTEMS

Probabilistic safety verification problem is required to handle the interplay between the continuous consecution involved with ODE and randomness of initial set. Meanwhile, there is no explicit analytic expression for the safe initial state set $\mathcal{I}$, which results in that the exact probability for the probabilistic safety verification problem is impossible to achieve. To make this problem tractable, our goal is computing a suitable subset $\Theta \subset \mathcal{I}$ such that any trajectory starting from Θ will never enter the unsafe region X_u. By integrating probability measures of random variables on the subset Θ, we then obtain the lower bound of the exact safety probability.

In the conventional hybrid system, the concept of barrier certificate plays an important role in safety verification due to its less computational difficulty than reachable set computation. Encouraged by the benefit of barrier certificate, we derive it to attack the probabilistic safety verification of stochastic hybrid systems.

Definition 3.1 (Probabilistic Barrier Certificate). Let $\mathbf{SH} : \langle L, X, F, \Psi, E, G, R, \Omega, \ell_0 \rangle$ be a semi-algebraic stochastic hybrid system with an unsafe region X_u. Let $p \in (0, 1]$. Let $\lambda_\ell(\mathbf{x})$ be given polynomials for all $\ell \in L$, and $\gamma_e(\mathbf{x})$ be given nonnegative polynomials for all $e \in E$. If there exists a Borel initial state set Θ and for each location $\ell \in L$ there exists a polynomial $B_\ell(\mathbf{x}) \in \mathbb{R}[\mathbf{x}]$ for each location $\ell \in L$, which satisfy the following conditions:

(i) $P(x \in \Theta) \geq p$,
(ii) $B_{\ell_0}(\mathbf{x}) \geq 0 \; \forall \mathbf{x} \in \Theta$,
(iii) $\dot{B}_\ell(\mathbf{x}) - \lambda_\ell(\mathbf{x}) B_\ell(\mathbf{x}) > 0 \; \forall \mathbf{x} \in \Psi(\ell)$, here $\dot{B}_\ell(\mathbf{x})$ denotes the Lie-derivative of $B_\ell(\mathbf{x})$ along the vector field $\mathbf{f}_\ell$, i.e., $\dot{B}_\ell(\mathbf{x}) = \sum_{i=1}^{n} \frac{\partial B_\ell}{\partial x_i} \cdot f_{\ell,i}(\mathbf{x})$,
(iv) $B_{\ell'}(\mathbf{x}') - \gamma_e(\mathbf{x}) B_\ell(\mathbf{x}) \geq 0 \; \forall \mathbf{x}' = R_e(\mathbf{x}) \;\; \forall \mathbf{x} \in G_e, \forall e = (\ell, \ell') \in E$,
(v) $B_\ell(\mathbf{x}) < 0 \; \forall \mathbf{x} \in X_u(\ell)$,

then $B_\ell(\mathbf{x})$ is a *p-barrier certificate* (p-BC) at the location ℓ, and $\mathbf{SH}$ is called p-safe.

Intuitively Definition 3.1 indicates that the conditions signify that $B_\ell(\mathbf{x})$ is the barrier certificate of $\mathbf{SH}$ with a specific initial state set Θ. As a consequence, $\Theta \subseteq \mathcal{I}$, which yields that p is the lower bound of the exact probability of safety of $\mathbf{SH}$. From Definition 3.1, it is seen that the main difference between the definitions of barrier certificates of conventional hybrid systems and stochastic ones

is that the p-BC of a stochastic hybrid system is associated with a specific Borel initial state set. Hence a key difficulty is how to compute a suitable initial state set Θ such that the lower bound p is as close as possible to the exact probability. In Section 3 we design an approximation scheme for the safety of stochastic hybrid systems by means of generating the p-barrier certificates associated with safe initial subset.

4 PROBABILISTIC BARRIER CERTIFICATE GENERATION

We wrote earlier that the safe initial state set $\mathcal{I}$ is unattainable. To alleviate this computational intractability, a relax surrogate is to compute a suitable approximation of $\mathcal{I}$. The basic idea is to introduce a parametric set $\Theta(\alpha)$ as the approximation of $\mathcal{I}$, and then establish a polynomial optimization problem yielded from the constraints of probabilistic barrier certificate generation, proceeds by solving the resulted polynomial optimization problem to produce the lower bound of the exact safety probability in association with the probabilistic barrier certificate.

This section develops an efficient algorithm for producing a probabilistic barrier certificates of stochastic hybrid systems with unsafe region, which also enjoys absolute safety probability guarantees. Following the spirit of barrier certificates, we propose a novel procedure called probabilistic barrier certificate generation (PBCG) adopting a adaptive approximation for the initial state set. Informally, PBCG proceeds in two stages:

(1) **Parameterize Initial State Set:** construct a parametric set $\Theta(\alpha)$ from the initial distribution Ω of **SH**.
(2) **Generate Probabilistic Barrier Certificate:** compute a probabilistic barrier certificate by means of solving the bilinear matrix inequalities (BMI) yielded from the conditions in Definition 3.1 and $\Theta(\alpha)$.

Three remarks are in order:

- Firstly, in order for the parametric initial set $\Theta(\alpha)$ to approximate the initial distribution appropriately, we need to seed it with the feature of the initial distribution Ω. The key idea is, by exploiting the feature of the probability density function of Ω, to build the corresponding template $\Theta(\alpha)$ such that the probability that the random initial variable lies in $\Theta(\alpha)$, say $P(\mathbf{x} \in \Theta(\alpha))$, is as large as possible when the parameter α is fixed. It is worth noting that different distributions have diverse features. As we shall see later, the main point is how to diagnose the inherent feature of the specific distribution to build its suitable template.
- Secondly, in order to enlarge the computed safe initial state set $\Theta(\alpha)$, we maximize α while imposing the constraints of probabilistic barrier certificate. The problem for generating probabilistic barrier certificates while maximizing α can be cast as an optimization problem with a bilinear matrix inequalities (BMI) constraint.
- Finally, we can compute the probability $P_\alpha = P(\mathbf{x} \in \Theta(\alpha))$ once the parameter α is obtained. Furthermore, the existence of barrier certificates indicates that any trajectory starting from $\Theta(\alpha)$ will never enter the unsafe set, namely, $\Theta(\alpha) \subset \mathcal{I}$. Hence, P_α is the lower bound of the exact safety probability of the system, i.e., $P_\alpha \leq P_{\text{safe}}$. In words, our algorithm comes with provable probability guarantees, which are particularly important in formal verification of stochastic hybrid systems.

A procedure called PBCG is summarized in Algorithm 1, and a specification of Algorithm 1 is deferred to Section 4.1 and Section 4.2.

ALGORITHM 1: PBCG: Probabilistic Barrier CertificatesGeneration

Input: **SH**: a stochastic hybrid system with an unsafe region
Output: $\{B_\ell(\mathbf{x})\}$: the barrier certificate,
P_α: the lower bound of safety probability P_{safe}.

1 $\Theta(\alpha) \leftarrow genTemplate(\Omega)$;
2 $\{B_\ell(\mathbf{x})\}, P_\alpha \leftarrow genBarrierCertificate(\mathbf{SH}, \Theta(a))$;
3 **return** $\{B_\ell(\mathbf{x})\}, P_\alpha$.

4.1 Parameterize Initial State Set

Faced with the inability to compute the exact safety probability P_{safe} for a stochastic hybrid system, our solution is to compute its lower bound P_α by computing $\Theta(\alpha)$, which is the approximation of the safe initial state set $\mathcal{I}$. This simplifies the problem considerably, but we run into a new difficulty: how to select a suitable initial state set template $\Theta(\alpha)$ for the initial distribution Ω from the stochastic hybrid system.

In order to enlarge P_α by choice of $\Theta(\alpha)$, we define a parametric compact set

$$\Theta(\alpha) := \{\mathbf{x} \in \mathbb{R}^n | \theta_j(\mathbf{x}, \alpha) \le 0, j = 1, \ldots, k\}, \tag{5}$$

and then maximize α while imposing the constraint for the existence of probabilistic barrier certificates. To our purpose, the principle for selecting a specific template of $\Theta(\alpha)$ in (5) is how to enlarge the probability P_α for the fixed α. Benefiting from the property of the probability density function, an impulse on choice of the template is that $\Theta(\alpha)$ should lie in the region with the large value of probability density function. Concretely, given a general distribution Ω associated with the probability density function $f(\mathbf{x})$ and the threshold variable α, we can select the template of (5) by taking the form $\{\mathbf{x} \in \mathbb{R}^n | f(\mathbf{x}) \le \alpha\}$.

Consider different probability distributions have diverse probability density functions, that is, the unified form $f(\mathbf{x}) \le \alpha$ may lead to various parametric initial state sets. In what follows, we provides the parametric initial sate sets for several typical distributions as well as the computation formulas of the probability P_α.

[Exponential Distribution]. Let $x_1, \ldots, x_n$ be random variables which obey the independent exponential distributions, and the associated probability density functions are

$$f_i(x_i) = \lambda_i e^{-\lambda_i(x_i - \mu_i)}, \quad x_i \ge \mu_i;\ \lambda_i > 0,$$

where μ_i and λ_i are the location parameters and the rate parameters, i.e., $x_i - \mu_i \sim \mathcal{E}(\lambda_i), i = 1, \ldots, n$. So the joint density function of the random variable vector $\mathbf{x}$ is

$$f(\mathbf{x}) = \prod_{i=1}^{n} \lambda_i e^{-\lambda_i(x_i - \mu_i)},\ x_i \ge \mu_i,\ 1 \le i \le n.$$

Given a threshold likelihood β, $f(\mathbf{x}) \ge \beta$ can be expressed as

$$\left(\prod_{i=1}^{n} \lambda_i\right) e^{-\sum_{i=1}^{n} \lambda_i(x_i - o_i)} \ge \beta, \quad x_i \ge \mu_i,\ 1 \le i \le n,$$

which is equivalent to

$$\sum_{i=1}^{n} \lambda_i(x_i - \mu_i) \le -\ln \frac{\beta}{\prod_{i=1}^{n} \lambda_i}, \quad x_i \ge \mu_i,\ 1 \le i \le n.$$

Let $\alpha = -\ln \frac{\beta}{\prod_{i=1}^{n} \lambda_i}$, we select the parametric initial state set $\Theta_e(\alpha)$ below for the independent exponential distribution

$$\Theta_e(\alpha) = \left\{ \mathbf{x} \in \mathbb{R}^n | \sum_{i=1}^{n} \lambda_i (x_i - o_i) \leq \alpha,\ x_i \geq \mu_i,\ 1 \leq i \leq n \right\}. \tag{6}$$

The probability of $P(\mathbf{x} \in \Theta_e(\alpha))$ can be calculated by the following formula.

Theorem 4.1. *Let $x_1, \ldots, x_n$ be independent random variables which obey the exponential distributions respectively, i.e. $x_i - o_i \sim \mathcal{E}(\lambda_i)$. Let $\Theta_e(\alpha)$ be defined as in (6), then we have*

$$P(\mathbf{x} \in \Theta_e(\alpha)) = 1 - e^{-\alpha} - \sum_{i=2}^{n} \frac{\alpha^{n-1} e^{-\alpha}}{(i-1)!}. \tag{7}$$

[Uniform Distribution]. Let $x_1, \ldots, x_n$ be independent random variables, and for each $i, 1 \leq i \leq n$, x_i obeys the uniform distribution in the interval $[l_i, u_i]$, i.e., $x_i \sim \mathcal{U}(l_i, u_i)$, And the probability density function of x_i is

$$f_i(x_i) = \frac{1}{u_i - l_i}, \quad l_i \leq x_i \leq u_i.$$

So the joint density function of $\mathbf{x}$ is

$$f(\mathbf{x}) = \prod_{i=1}^{n} \frac{1}{u_i - l_i}, \quad l_i \leq x_i \leq u_i,\ 1 \leq i \leq n.$$

It is seen that the likelihood is equal in the area

$$\{\mathbf{x} \in \mathbb{R}^n | \ l_i \leq x_i \leq u_i,\ 1 \leq i \leq n\}.$$

Consequently, we can simplify to select the parametric initial state set as a specific n-dimensional hypercube, which is written as

$$\Theta_u(\alpha) = \{\mathbf{x} \in \mathbb{R}^n | -\alpha r_i \leq x_i - c_i \leq \alpha r_i, i = 1, \ldots, n\}. \tag{8}$$

where $c_i = \frac{l_i + u_i}{2}$ and $r_i = \frac{u_i - l_i}{2}$ for each i. Moreover, the probability for $P(\mathbf{x} \in \Theta_u(\alpha))$ can be computed by means of the following formula.

Theorem 4.2. *Let $x_1, \ldots, x_n$ be independent random variables which obey the uniform distribution respectively, i.e. $x_i \sim \mathcal{U}(l_i, u_i)$. Define Θ_u as in (8), then we have*

$$P(\mathbf{x} \in \Theta_u(\alpha)) = \alpha^n. \tag{9}$$

[Normal Distribution]. Let $x_1, \ldots, x_n$ be random variables,which obey the joint normal distribution with the expectation vector μ and the covariance matrix Σ, and $\mu \in X$. Consider the joint density function of $\mathbf{x}$

$$f(\mathbf{x}) = \frac{1}{\sqrt{(2\pi)^n |\Sigma|}} e^{-\frac{1}{2}(\mathbf{x}-\mu)^T \Sigma^{-1} (\mathbf{x}-\mu)},$$

where $|\Sigma|$ is the determinant of Σ. Given a threshold likelihood β, $f(\mathbf{x}) \geq \alpha)$ can be written as

$$\frac{1}{\sqrt{(2\pi)^n |\Sigma|}} e^{-\frac{1}{2}(\mathbf{x}-\mu)^T \Sigma^{-1} (\mathbf{x}-\mu)} \geq \beta,$$

which is equivalent to

$$(\mathbf{x} - \mu)^T \Sigma^{-1} (\mathbf{x} - \mu) \leq -2 \ln(\beta \sqrt{(2\pi)^n |\Sigma|}).$$

Let $\alpha = -2 \ln(\beta \sqrt{(2\pi)^n |\Sigma|})$, then we can choose the parametric initial state set by taking the form:

$$\Theta_n(\alpha) = \{\mathbf{x} \in \mathbb{R}^n | \ (\mathbf{x} - \mu)^T \Sigma^{-1} (\mathbf{x} - \mu) \leq \alpha\}. \tag{10}$$

The probability $P(\mathbf{x} \in \Theta_n(\alpha))$ can also be computed from below.

THEOREM 4.3. *Let* $\mathbf{x}$ *be random variable vector which obeys the joint normal distribution, i.e.* $\mathbf{x} \sim \mathcal{N}_n(\mu, \Sigma)$. *Let* $\Theta_n(\alpha)$ *be defined as in (10), then we have*

$$P(\mathbf{x} \in \Theta_n(\alpha)) = \int_0^{\alpha} \frac{v^{(n-2)/2} e^{-v/2}}{2^{n/2}\Gamma(n/2)} dv, \tag{11}$$

where Γ *is Euler Gamma function.*

Remark 1. When the covariance Σ is diagonal, the general joint normal distribution $\mathcal{N}_n(\mu, \Sigma)$ degenerates to independent normal distribution, namely, $x_i \sim \mathcal{N}(\mu_i, \sigma_i^2)$ for each i, where μ_i is the i-th element of μ, and σ_i^2 is the i-th diagonal element of Σ. Hereafter we use $\mathcal{N}$ and $\mathcal{JN}$ to distinguish the independent normal distribution and joint normal distribution.

4.2 Generate Barrier Certificates

Having the parameterized initial state set $\Theta(\alpha)$ customized for the given initial distribution in Section 4.1, we now consider how to compute the safety probability of a semi-algebraic stochastic hybrid system **SH** via p-barrier certificate generation. In order to enlarge the safety probability p_α by choice of the p-barrier certificate $B_\ell(\mathbf{x})$, we maximize α in the initial state set $\Theta(\alpha)$ while imposing the constraints (ii-v) in Definition 3.1. This is written as an optimization problem

$$\left.\begin{array}{ll} \alpha^* = \max\limits_{\alpha, B_\ell} \alpha & \\ \text{s.t.} \quad B_{\ell_0}(\mathbf{x}) \geq 0 \, \forall \mathbf{x} \in \Theta(\alpha), & \\ \quad \dot{B}_\ell(\mathbf{x}) - \lambda_\ell(\mathbf{x}) B_\ell(\mathbf{x}) > 0 \forall \mathbf{x} \in \Psi(\ell), & \\ \quad B_{\ell'}(\mathbf{x}') - \gamma_e(\mathbf{x}) B_\ell(\mathbf{x}) \geq 0 \, \forall \mathbf{x}' = R_e(\mathbf{x}) \forall \mathbf{x} \in G_e, & \\ \quad B_\ell(\mathbf{x}) < 0 \, \forall \mathbf{x} \in X_u(\ell). & \end{array}\right\} \tag{12}$$

A set of functions $\{B_\ell(\mathbf{x})\}$, satisfying the constraints in (12), is a barrier certificate of state that separates reachable states of a system starting with the initial states in $\Theta(\alpha)$ from its unsafe region $X_u(\ell)$ for each location $\ell \in L$. By solving problem (12), we aim to seek the maximal initial set $\Theta(\alpha^*)$ from which the stochastic hybrid system **SH** is safe with respective to $X_u(\ell)$. It should be pointed out that there exists an objective function α in problem (12), which is different from the optimization problems with no objective functions stemed from the general barrier certificate generation of conventional hybrid systems in [8, 20, 26, 28].

The problem for computing the barrier certificate $\{B_\ell(\mathbf{x})\}$ with respective to $\Theta(\alpha^*)$ in (12) is an infinite dimensional problem. In order to make it amenable to polynomial optimization, the barrier certificate $\{B_\ell(\mathbf{x})\}$ should be restricted to a set of polynomials with a priori degree bound. Moreover, Sum-of-Squares (SOS) relaxation technique is applied to encode the optimization problem (12) as a SOS programming. In fact, given a basic semi-algebraic set $\mathbb{K}$ defined by:

$$\mathbb{K} = \{\mathbf{x} \in \mathbb{R}^n \mid g_1(\mathbf{x}) \geq 0, \ldots, g_s(\mathbf{x}) \geq 0\},$$

where $g_j \in \mathbb{R}[\mathbf{x}], 1 \leq j \leq s$, a sufficient condition for the nonnegativity of the given polynomial $f(\mathbf{x})$ on the semi-algebraic set $\mathbb{K}$ is provided as

$$(f(\mathbf{x}) = \sigma_0(\mathbf{x}) + \sum_{i=1}^{s} \sigma_i(\mathbf{x}) g_i, \text{ with } \deg(\sigma_i) \leq D) \wedge (\sigma_i \in \Sigma[\mathbf{x}], \ 1 \leq i \leq s), \tag{13}$$

where $\Sigma(\mathbf{x}) \subset \mathbb{R}[\mathbf{x}]$ is the space of SOS polynomials. Thus, the representation (13) ensures that the polynomial $f(\mathbf{x})$ is nonnegative on the given semi-algebraic set $\mathbb{K}$. Given the initial distribution Ω, recall the representation of the parametric initial state set $\Theta(\alpha)$:

$$\Theta(\alpha) := \{\mathbf{x} \in \mathbb{R}^n | \theta_j(\mathbf{x}, \alpha) \leq 0, \quad 1 \leq j \leq k\}.$$

Based on the above observation, the problem for computing safety probability of **SH** can be transformed into the following problem

$$\left.\begin{array}{ll} \hat{a} = \max\limits_{\alpha, B_\ell} \alpha & \\ \text{s.t.} & B_{\ell_0}(\mathbf{x}) + \sigma_j(\mathbf{x})\theta_j(\mathbf{x}, \alpha) \in \Sigma[\mathbf{x}], \\ & \dot{B}_\ell(\mathbf{x}) - \lambda_\ell(\mathbf{x})B_\ell(\mathbf{x}) - \phi_\ell(\mathbf{x})\psi_\ell(\mathbf{x}) - \epsilon_{\ell,1} \in \Sigma[\mathbf{x}], \\ & B_{\ell'}(R_e(\mathbf{x})) - \gamma_e(\mathbf{x})B_\ell(\mathbf{x}) - \vartheta_e(\mathbf{x})g_e(\mathbf{x}) \in \Sigma[\mathbf{x}], \\ & -B_\ell(\mathbf{x}) - \epsilon_{\ell,2} - \mu_\ell(\mathbf{x})\zeta_\ell(\mathbf{x}) \in \Sigma[\mathbf{x}], \end{array}\right\} \tag{14}$$

where $\epsilon_{\ell,1} > 0$, $\epsilon_{\ell,2} > 0$, the entries of $\sigma_j(\mathbf{x})$, $\gamma_e(\mathbf{x})$, $\vartheta_e(\mathbf{x})$, and $\mu_\ell(\mathbf{x})$ are SOSes. Clearly, the feasibility of the constraints in (14) is sufficient to imply that the feasibility of the constraints in (12). Consequently, it is seen that $\hat{a} \leq a^*$.

It is worth noting that the problem (14) is a special SOS program which puts the maximal size of the chosen region template as the objective function and encodes the verification conditions of probabilistic barrier certificates as constraints. Such an optimization problem is certainly different from the constraint solving problem arising from the generation of general barrier certificates of deterministic hybrid systems [28].

The degree bound for the multiplier polynomials is exponential with the number of variables $\mathbf{x}$ and the degrees of the polynomials appearing in the semi-algebraic sets. To avoid high computational complexity, we set up a truncated SOS programming for (14) by fixing a *priori* (much smaller) degree bound $2e$, with $e \in \mathbb{Z}_+$, of all the unknown multiplier polynomials.

As stated in [20, 28], a significant progress was made in choosing the fixed polynomials $\lambda_\ell(\mathbf{x})$ and nonnegative polynomials $\gamma_e(\mathbf{x})$. However, the SOS program (14) is bilinear in the parameter α and the unknown multiplier $\sigma_\ell(\mathbf{x})$, yielding a particular non-convex bilinear matrix inequalities (BMI) problem. Fortunately, a Matlab package PENBMI solver [21], which combines the (exterior) penalty and (interior) barrier method with the augmented Lagrangian method, can be applied directly to obtain the numerical solution of the problem (14). Nevertheless, the nonconvexity is not to be taken lightly, and any numerical attempt to compute must itself treated as a lower bound.

Finally, the solution to problem (14) yields a barrier certificate $\{B_\ell(\mathbf{x})\}$, which can ensure that the stochastic hybrid system **SH** is safe, with respective to the determined initial state set $\Theta(\hat{\alpha})$. It also means that the stochastic hybrid system **SH** with an initial distribution Ω is p-safe, where p is the lower bound of $P(x \in \Theta(\hat{a}))$, specified by the formulas given in Theorem 4.1–4.3.

5 EXPERIMENTS

In this section, we first show the principle of proposed barrier certificate based method for probabilistic safety verification by a stochastic continuous system and then evaluates the effectiveness of the computational method by comparing it with random testing.

Example 5.1. [28] Consider the following stochastic continuous system. The dynamic vector field is

$$f(\mathbf{x}) = \begin{bmatrix} x_2 \\ -x_1 + \frac{1}{3}x_1^3 - x_2 \end{bmatrix},$$

with the location invariant

$$\Psi = \{\mathbf{x} \in \mathbb{R}^2 | -6 \leq x_1, x_2 \leq 6\}.$$

The initial distribution is

$$\Omega : x_1 \sim \mathcal{N}(1.5, 0.64), x_2 \sim \mathcal{N}(0, 1.28).$$

The unsafe set

$$X_u = \{\mathbf{x} \in \mathbb{R}^2 | (x_1 + 1)^2 + (x_2 + 1)^2 \leq 0.16\}.$$

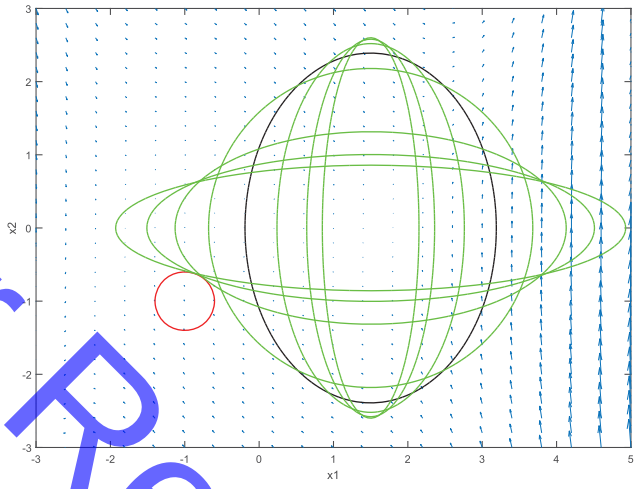

Fig. 1. Safe initial states found by ellipsoid templates.

We try to explore the safety probability of the system. Following our method, for the ellipsoid template, the proportion of radii along x_1 and x_2 and the center of the ellipsoid were set to $d = 1/\sqrt{2}$ and (1.5,0) respectively. By solving the corresponding optimization problem (14), we can obtain $P_\alpha = 0.8926$, which is the lower bound of the exact safety probability P_{safe}.

A set of ellipsoids constructed with random proportion of radii and random length of radii are placed in the verification conditions of barrier certificates, and those satisfying the conditions are recorded. From the testing, the obtained safety probabilities range from 0.5210 to 0.9129.

Figure 1 shows some safe initial regions obtained by the random testing as well as the one found by our method. Here, the blue arrows represent the vector field in the location invariant, the red circle is the unsafe region of the system, the green ellipsoids are the largest safe initial regions of a specific proportion of radii, and the black ellipsoid is the initial state set computed by our method. It can be seen from the figure that the green ellipsoid is very close to the biggest green one, which corresponds to the largest safety probability.

The characterization of random initial states is orthogonal to the other random characterizations studied in the related work. The following example shows that our method can be directly combined with the one proposed in [27] to settle the safety verification problem of stochastic hybrid systems where randomness occurs in both initial conditions and dynamic equations.

Example 5.2. [27] Consider the following stochastic continuous system

$$\begin{bmatrix} dx_1(t) \\ dx_2(t) \end{bmatrix} = \begin{bmatrix} x_2 dt \\ (-x_1(t) - x_2(t) - 0.5x_1^3(t))dt + 0.1dw(t) \end{bmatrix}$$

where w is an 1-dimensional Wiener process. Suppose that the local invariant is

$$\Psi = \{\mathbf{x} \in \mathbb{R}^2 : -3 \leq x_1, x_2 \leq 3, x_1^2 + x_2^2 \geq 0.25\},$$

the initial distribution is

$$x_1 \sim \mathcal{U}([-2.1, -1.9]),\ x_2 \sim \mathcal{U}([-0.1, 0.1]),$$

and the unsafe set

$$X_u = \{\mathbf{x} \in \mathbb{R}^2 : x_2 \geq 2.25\}.$$

Table 1. Safety Probability Comparison

Ex.	n	$\|L\|$	Ω	$d(B)$	P_α	P_{rec}	P_{ell}
C1	4	1	$\mathcal{U}$	2	0.816	[0.182,0.782]	[0.515,0.989]
			$\mathcal{N}$	2	0.829	[0.163,0.411]	[0.412,0.829]
			$\mathcal{E}$	4	0.849	[0.565,0.854]	[0.756,0.892]
			$\mathcal{TN}$	2	0.805	[0.180,0.434]	[0.416,0.817]
C2	6	1	$\mathcal{U}$	2	0.942	[0.350,0.942]	[0.137,0.815]
			$\mathcal{N}$	2	0.948	[0.372,0.980]	[0.147,0.903]
			$\mathcal{E}$	2	0.958	[0.317,0.896]	[0.590,0.990]
			$\mathcal{TN}$	2	0.978	[0.373,0.981]	[0.148,0.898]
C3	6	1	$\mathcal{U}$	4	0.833	[0.167,0.833]	[0.137,0.330]
			$\mathcal{N}$	4	0.998	[0.265,0.999]	[0.275,0.991]
			$\mathcal{E}$	4	0.933	[0.149,0.997]	[0.222,0.999]
			$\mathcal{TN}$	4	0.998	[0.266,0.999]	[0.275,0.987]
H1	2	2	$\mathcal{U}$	2	0.792	[0.343,0.792]	[0.717,0.809]
			$\mathcal{N}$	2	0.886	[0.337,0.800]	[0.663,0.714]
			$\mathcal{E}$	2	0.929	[0.417,0.879]	[0.431,0.882]
			$\mathcal{TN}$	2	0.845	[0.338,0.801]	[0.662,0.715]
H2	2	2	$\mathcal{U}$	2	0.825	[0.260,0.905]	[0.321,0.957]
			$\mathcal{N}$	2	0.883	[0.267,0.922]	[0.352,0.882]
			$\mathcal{E}$	2	0.979	[0.145,0.911]	[0.142,0.901]
			$\mathcal{TN}$	2	0.908	[0.268,0.922]	[0.352,0.881]

By combining our approach with the barrier certificate based method proposed in [27], we can obtain that the lower bound of the safety probability is 0.8104.

The effectiveness of our method should be further investigated by more examples. Here, we chose five examples (three stochastic continuous systems and two stochastic hybrid systems) as benchmarks and compared the safety probabilities our method returned with those derived from random testing. The random testing is performed with the following configuration:

- Only involved two types of template: an ellipsoid and a rectangle.
- The center of the template was set to the mean of the initial distribution, the same as our method.
- The portion of radii or and the length of radii were randomly generated.
- The time spent in random testing was set to 3 hours as the maximal time taken by ours was less than 3 minutes.

To further evaluate the relation between the type of template and the stochastic distribution of initial states, for each example, we tested four types of stochastic distribution: independent exponential distribution, independent normal distribution, independent uniform distribution and joint normal distribution. Details about the examples can be found in Appendix B. Here, the SDP problems were solved by the PENBMI solver [21]. And the experiments were performed on Intel(R) Core(TM) at 3.40GHz with 8GB of memory under Windows. Table 1 lists the result.

In Table 1, n and $|L|$ denote the number of the system variables and the number of the locations; Ω denotes the initial distribution; $d(B)$ denotes the degrees of the barrier certificates obtained from SDP solvers; P_α denotes the safety probability computed by our PBCG procedure. P_{rec} and P_{ell} denote the safety probability computed by random testing using rectangle template and

ellipsoid template respectively. Each pair records an interval of the minimal and the maximal safety probability being found.

The effectiveness of our method can be investigated line by line. It can be seen from the table that our approach performs better than rectangle template in almost all the cases. As for the ellipsoid template, among 20 cases, there are 7 cases where our approach performs better, 7 cases where the difference is within 2%, 4 cases where the difference is within 10%. Besides, considering that our methods use only less than 1/60 time in producing the result, it is safe to say that our method is significantly more effective.

As for the initial distribution's impact on the template, we can see that faced with the normal distribution and the joint normal distribution, among 10 cases, our template performs better in 3 cases, similar to the others in 3 cases and slightly worse in 4 cases. Faced with the exponential distribution, our template is better in 2 out of the 5 cases. Faced with uniform distribution, the ellipsoid template always achieve the best. In summary, except for the uniform distribution, our templates perform better than the other two templates, meaning that the guideline that always tries to lie in the region with the large value of probability density function does take effects. As for the uniform distribution, as the probability is identical everywhere in the support, in the current setting, our template can not achieve higher probability. Such a result may be considered as an evidence to support our guideline from the opposite direction.

It is worthy pointing out why random testing may give higher safety probability. In fact, the safety probability is determined by both the stochastic distribution of initial states and the distribution of dangerous initial states. For a given verification problem, the former is known while the latter is unknown acting as the verification target. In our method, the knowledge of the initial distribution is used in the construction of the optimal template. However, if the distribution of dangerous initial states is egregious, for example, dangerous initial states are concentrated on a specific area near the mean, the shape of our suggested template will be quite different from the real safe region of initial states, resulting in a relatively conservative safe region of initial states. In comparison, the random testing may have the chance to approach the real safe region at the cost of a big number of trials, but the whole testing process is uncontrollable.

6 RELATED WORK

To model the random phenomenon in many modern application areas of hybrid systems, there have been several notions of stochastic hybrid systems proposed in recent years [1, 7, 11, 17, 22, 27, 32, 36, 38]. Based on the point where the randomness is integrated in, they fall into three categories. The first class focus on stochastic discrete jumps. That is, deterministic transitions are replaced by probability distributions over transitions. In [22], authors consider timed automata with probabilistic discrete transitions. Then the probabilistic timed automata are extended to probabilistic hybrid automata in [12, 38]. The second class introduces randomness into continuous behaviors. In [9], authors treat affine hybrid systems with uncertainty vector field and solve the infinite time reachability. In [27], continuous behaviors are modeled as stochastic differential equations (SDE) instead of the ordinary differential equations (ODE) in a usual hybrid automata. The third class considers random initial conditions. In [32], the authors studied the safety verification problem of hybrid systems with random initial conditions. In [6, 17], the more general model with both stochastic continuous and discrete behaviors are studied based on the technique of Markov decision process (MDP).

There are some approaches that deal with the probabilistic safety verification problem of stochastic hybrid systems [1, 32, 36]. In [1], a method that combines numerical approximation with model checking techniques is proposed in which the stochastic hybrid system is firstly approximated by a finite state Markov chain and then the latter is verified by model checker. However, the

model they studied is based on discrete time, while in this work, the time variable is continuous. In [36], the SReach tool tries to combine statistical techniques with δ – complete procedures to solve the probabilistic bounded reachability problem. But it can treat the stochastic hybrid system in the paper, whereas only provides the statistical guarantees in a finite time horizon. Strictly speaking, the semantics of statistical guarantees does not fully comply with the usual semantics of verification, i.e., exhausting all the states which stands for absolutely correct. In [32], the authors developed a tool ProbReach to address the same problem for the similar system. The main idea is to first partition the state space into small intervals and then verify all of them one by one. After that, the safety probability is computed as the sum of the probabilities of all the "safe" intervals. In order to get an acceptable result, ProbReach always needs fine partition granularity, which means heavy computation efforts are required. In addition, as a reachable set computation based technique is used for verification, it can only check a limited number of discrete steps.

In contrast, our probabilistic barrier certificates generation approach can guarantee the absolute correctness in an infinite time horizon by enabling the comparison of the computed lower bound of safety probability with the threshold of acceptable safety probability. To the best of our knowledge, for the probabilistic safety verification of hybrid systems with stochastic initial states, it is the first work providing the absolute guarantees in an infinite time horizon.

Since the characterization, stochastic initial states, is orthogonal to the other two random characterizations: stochastic discrete jumps and stochastic continuous behaviors, it is possible to combine our approach with others to treat stochastic hybrid systems with more than one stochastic features. As shown in Example 5.2, the safety verification problem of stochastic hybrid systems with both stochastic differential equations and random initial conditions can be treated by directly combining our approach with that proposed in [27].

7 CONCLUSION

In this paper, we have presented a new barrier certificate based method for verifying probabilistic safety property of stochastic nonlinear hybrid systems. The key distinguishing feature of barrier certificate based method is that it can guarantee the system to be absolute safe in an infinite time horizon. Taking advantage of the characteristics of initial states, the template configurations of initial state sets for three typical distribution are proposed which help to build the optimization problem by maximizing the safe probability with the conditions of barrier certificates. The SOS relaxation based method can yield the solution of the optimization problem, which gives the lower bound of exact safety probability of stochastic nonlinear hybrid systems. Rather than statistical model checking, our method can provide absolute safety probability guarantees. We also demonstrated by the experiments on some benchmarks to show our method is efficient and practical. We will study the combination of our method with related work to settle the safety verification problem of general stochastic hybrid systems in the future.

APPENDIXES

A PROOF OF THEOREMS

Proof of Lemma 2.4. We need to prove two cases of C_i: the discrete consecution and the continuous consecution. We first consider the first case: $R^{-1}_{(\ell_i,\ell_{i+1})}(A)$ is Borel. It is known that the inverse image of an open set under a continuous function is also open. Since Borel sets can be regarded as the countable union and complement of open sets, $R^{-1}_{(\ell_i,\ell i+1)}(A)$ is Borel.

Next, let us prove the other case: the continuous consecution. For any open set U, from (2) we have

$$G^{-1}_{\ell}(U) = \bigcup_{t\geq 0} \mathbf{x}^{-1}_{\ell}(U,t).$$

Since $\mathbf{x}_\ell$ is continuous for x and U is open, $\mathbf{x}_\ell^{-1}(U,t)$ is also open for any $t \geq 0$, which leads to $G_{\ell_i}^{-1}(A)$ is a Borel set. □

Proof of Theorem 4.1. For new variables

$$\mathbf{y} = [y_1, \ldots, y_n]^T,$$

we define the map:

$$\phi : \mathbb{R}[x_1, \ldots, x_n] \to \mathbb{R}[y_1, \ldots, y_n],$$

where

$$y_i = \lambda_i(x_i - \mu_i), \quad 1 \leq i \leq n.$$

Then we have

$$\phi(\Theta_e(\alpha)) = \{\mathbf{y} \in \mathbb{R}^n | \sum_{i=1}^{n} y_i \leq \alpha, \quad y_i \geq 0, 1 \leq i \leq n\},$$

and the corresponding Jacobian determinant

$$det(J(y)) = det(diag(\lambda_1^{-1}, \ldots, \lambda_n^{-1})) = \left(\prod_{i=1}^{n} \lambda_i\right)^{-1}.$$

Thus,

$$P(\mathbf{x} \in \Theta_e(\alpha)) = \int_{\mathbf{y} \in \phi(\Theta_e(\alpha))} \prod_{i=1}^{n} e^{-y_i} dy_n \cdots dy_1.$$

Let $g_n(\alpha) = \int_{\mathbf{y} \in \phi(\Theta(a))} \prod_{i=1}^{n} e^{-y_i} dy_n \cdots dy_1$, then we have

$$\begin{aligned} g_n(\alpha) &= \int_{\sum_{i=1}^{n-1} y_i \leq \alpha, y_i \geq 0, 1 \leq i \leq n-1} \left(\int_0^{\alpha - \sum_{i=1}^{n-1} y_i} \prod_{i=1}^{n} e^{-y_i} dy_n \right) \cdots dy_1 \\ &= \int_{\sum_{i=1}^{n-1} y_i \leq \alpha, y_i \geq 0, 1 \leq i \leq n-1} (-e^{-\alpha} + e^{\sum_{i=1}^{n-1} y_i}) dy_{n-1} \cdots dy_1 \\ &= -\frac{\alpha^{n-1}}{n!} e^{-\alpha} + g_{n-1}(\alpha). \end{aligned}$$

The above recursive relation of $g_i(\alpha)$ yields that

$$\begin{aligned} P(\mathbf{x} \in \Theta_e(\alpha)) &= -\sum_{i=2}^{n} \frac{\alpha^{i-1}}{i!} e^{-\alpha} + g(1) \\ &= -\sum_{i=2}^{n} \frac{\alpha^{i-1}}{i!} e^{-\alpha} + 1 - e^{-\alpha}, \end{aligned}$$

which is the desired result. □

Proof of Theorem 4.2. Since $x_1, \ldots, x_n$ are the independent random variables, the following equation holds.

$$P(\mathbf{x} \in \Theta_u(\alpha)) = \prod_{i=1}^{n} P(-\alpha r_i \leq x_i - c_i \leq \alpha r_i).$$

By the cumulative distribution function of the uniform distribution, it is followed that

$$\prod_{i=1}^{n} P(-\alpha r_i \leq x_i - c_i \leq \alpha r_i) = \alpha^n,$$

namely, $P(\mathbf{x} \in \Theta_u(\alpha)) = \alpha^n$. □

Proof of Theorem 4.3. We refer to [4] for the proof. □

B BENCHMARK EXAMPLES

Example C1. [30]

$$f(\mathbf{x}) = \begin{bmatrix} -x_1 + x_2^3 - 3x_3x_4 \\ -x_1 - x_2^3 \\ x_1x_4 - x_3 \\ x_1x_3 - x_4^3 \end{bmatrix}.$$

- The local invariant Ψ: $\{\mathbf{x} \in \mathbb{R}^4 : -2 \le x_1, x_2, x_3, x_4 \le 2\}$;
- The initial distribution Ω:
  $-x_1, x_2, x_3 \sim \mathcal{U}([-0.84, 0.84])$,
  $x_4 \sim \mathcal{U}([-0.28, 0.28])$,
  $-x_1, x_2, x_3 \sim \mathcal{N}(0, 0.36)$, $x_4 \sim \mathcal{N}(0, 0.04)$,
  $-x_1 + 0.4, x_2 + 0.4, x_3 + 0.4 \sim \mathcal{E}(2.5)$,
  $x_4 + 0.2 \sim \mathcal{E}(5)$,
  $$\mathbf{x} \sim \mathit{JointN}_4\left(\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0.36 & 0.04 & 0.04 & 0.04 \\ 0.04 & 0.36 & 0.04 & 0.04 \\ 0.04 & 0.04 & 0.36 & 0.04 \\ 0.04 & 0.04 & 0.04 & 0.04 \end{bmatrix}\right);$$
- The unsafe set X_u: $\{\mathbf{x} \in \mathbb{R}^4 : -1 \le x_1, x_2, x_3, x_4 \le -0.5\}$.

Example C2. [5]

$$f(\mathbf{x}) = \begin{bmatrix} -x_1^3 + 4x_2^3 - 6x_3x_4 \\ -x_1 - x_2 + x_5^3 \\ x_1x_4 - x_3 + x_4x_6 \\ x_1x_3 + x_3x_6 - x_4^3 \\ -2x_2^3 - x_5 + x_6 \\ -3x_3x_4 - x_5^3 - x_6 \end{bmatrix}.$$

- The local invariant Ψ: $\{\mathbf{x} \in \mathbb{R}^6 : 0 \le x_1, x_2, x_4, x_5, x_6 \le 15, 2 \le x_3 \le 15\}$;
- The initial distribution Ω:
  $-x_1, x_5 \sim \mathcal{U}([0, 8]), x_3 \sim \mathcal{U}([2, 5])$,
  $x_2, x_4 \sim \mathcal{U}([0, 7]), x_6 \sim \mathcal{U}([2.3, 4.5])$,
  $-x_1, x_5 \sim \mathcal{N}(4, 0.72), x_6 \sim \mathcal{N}(3.4, 0.09)$,
  $x_2, x_3, x_4 \sim \mathcal{N}(3.5, 0.18)$,
  $-x_1 + 3, x_5 + 3 \sim \mathcal{E}(1), x_6 + 3 \sim \mathcal{E}(2.5)$,
  $x_2 + 3, x_3 + 3, x_4 + 3 \sim \mathcal{E}(2)$,
  $$-\mathbf{x} \sim \mathit{JointN}_6\left(\begin{bmatrix} 4 \\ 3.5 \\ 3.5 \\ 3.5 \\ 4 \\ 3.4 \end{bmatrix}, \begin{bmatrix} 0.72 & 0.04 & 0.04 & 0.04 & 0.04 & 0.04 \\ 0.04 & 0.18 & 0.04 & 0.04 & 0.04 & 0.04 \\ 0.04 & 0.04 & 0.18 & 0.04 & 0.04 & 0.04 \\ 0.04 & 0.04 & 0.04 & 0.18 & 0.04 & 0.04 \\ 0.04 & 0.04 & 0.04 & 0.04 & 0.72 & 0.04 \\ 0.04 & 0.04 & 0.04 & 0.04 & 0.04 & 0.09 \end{bmatrix}\right);$$
- The unsafe set X_u: $\{\mathbf{x} \in \mathbb{R}^6 : (x_1 - 4.05)^2 + (x_2 - 4.15)^2 + (x_3 - 4.25)^2 + (x_4 - 4.35)^2 + (x_5 - 4.45)^2 + (x_6 - 4.55)^2 \le 0.05^2\}$.

Example C3. [34]

$$f(\mathbf{x}) = \begin{bmatrix} x_4 \\ x_5 \\ x_6 \\ -\frac{2}{3}x_1 + \frac{1}{3}x_1x_3 \\ \frac{1}{3}x_1 + \frac{2}{3}x_2 + \frac{1}{3}x_2x_3 \\ -4 + x_3^2 + 8x_5 \end{bmatrix}.$$

- The local invariant Ψ: $\{\mathbf{x} \in \mathbb{R}^6 : -4.5 \leq x_1, x_2, x_3, x_4, x_5, x_6 \leq 4.5\}$;
- The initial distribution Ω:
  $-x_1 \sim \mathcal{U}([-4, 4]), x_4 \sim \mathcal{U}([-0.5, 4.5]), x_3 \sim \mathcal{U}([-2.4, 2.4]),$
  $x_4 \sim \mathcal{U}([-2.5, 3.5]), x_5 \sim \mathcal{U}([0, 2]), x_6 \sim \mathcal{U}([-4, 0]),$
  $-x_1 \sim \mathcal{N}(0, 1), x_2 \sim \mathcal{N}(2, 0.36), x_3 \sim \mathcal{N}(0, 0.36),$
  $x_4 \sim \mathcal{N}(0.5, 0.56), x_5 \sim \mathcal{N}(1, 0.06), x_6 \sim \mathcal{N}(-2, 0.25),$
  $-x_1 + 0.5 \sim \mathcal{E}(2), x_2 - 1.7 \sim \mathcal{E}(3.33), x_3 + 0.3 \sim \mathcal{E}(3.33),$
  $x_4 + 0.125 \sim \mathcal{E}(2.67), x_5 - 0.875 \sim \mathcal{E}(8), x_6 + 2.25 \sim \mathcal{E}(4),$
  $-\mathbf{x} \sim \mathit{Joint}\mathcal{N}_6\left(\begin{bmatrix} 0 \\ 2 \\ 0 \\ 0.5 \\ 1 \\ -2 \end{bmatrix}, \begin{bmatrix} 1.00 & 0.04 & 0.04 & 0.04 & 0.04 & 0.04 \\ 0.04 & 0.36 & 0.04 & 0.04 & 0.04 & 0.04 \\ 0.04 & 0.04 & 0.36 & 0.04 & 0.04 & 0.04 \\ 0.04 & 0.04 & 0.04 & 0.56 & 0.04 & 0.04 \\ 0.04 & 0.04 & 0.04 & 0.04 & 0.06 & 0.04 \\ 0.04 & 0.04 & 0.04 & 0.04 & 0.04 & 0.25 \end{bmatrix}\right);$
- The unsafe set X_u: $\{\mathbf{x} \in \mathbb{R}^6 : (x_1 - 3)^2 + (x_2 - 3)^2 + (x_3 - 3)^2 + (x_4 - 3)^2 + (x_5 - 3)^2 + (x_6 - 3)^2 \leq 0.5^2\}$.

Example H1. Modified from [29]

$$f_1(\mathbf{x}) = \begin{bmatrix} -0.25x_1 \\ 0.25{+}0.25x_1{-}1.75x_2{+}0.8x_2^2 \end{bmatrix}, \quad f_2(\mathbf{x}) = \begin{bmatrix} -0.25x_1{+}0.25x_2 \\ 0.4{-}0.2x_1{-}0.25x_2 \end{bmatrix}.$$

- The local invariant:
  $$\Psi(\ell_1) : \{\mathbf{x} \in \mathbb{R}^2 | 4 \leq x_1 \leq 8, 0 \leq x_2 \leq 2\},$$
  $$\Psi(\ell_2) : \{\mathbf{x} \in \mathbb{R}^2 | 4 \leq x_1 \leq 6, 1 \leq x_2 \leq 2\};$$
- The initial distribution Ω:
  $-x_1 \sim \mathcal{U}([5.1, 5.9]),\ x_2 \sim \mathcal{U}([-0.15, 0.65]),$
  $-x_1 \sim \mathcal{N}(5.5, 0.48), x_2 \sim \mathcal{N}(0.25, 0.96),$
  $-x_1 - 5.25 \sim \mathcal{E}(2),\ x_2 + 0.25 \sim \mathcal{E}(4),$
  $-\mathbf{x} \sim \mathit{Joint}\mathcal{N}_2\left(\begin{bmatrix} 5.5 \\ 0.25 \end{bmatrix}, \begin{bmatrix} 0.48 & 0.12 \\ 0.12 & 0.96 \end{bmatrix}\right);$
- The initial location: ℓ_1;
- The guard condition G_{ℓ_1,ℓ_2}: $\{\mathbf{x} \in \mathbb{R}^2 : 0.99 \leq x_2 \leq 1\}$;
- The reset R_{ℓ_1,ℓ_2}: $x_1' = x_1 \wedge x_2' = 1$;
- The unsafe set $X_u(\ell_1)$: $\{\mathbf{x} \in \mathbb{R}^2 | (x_1 - 4.25)^2 + (x_2 - 0.25)^2 \leq 0.0625\}$.

Example H2. [37]

$$f_1(\mathbf{x}) = \begin{bmatrix} -x_1 + x_1x_2 \\ -x_2 \end{bmatrix}, \quad f_2(\mathbf{x}) = \begin{bmatrix} -x_1 + 2x_1^2x_2 \\ -x_2 \end{bmatrix}.$$

- The local invariant:

$$\Psi_{\ell_1} : \{\mathbf{x} \in \mathbb{R}^2 | -4 \le x_1 \le 0, -4 \le x_2 \le 4\},$$
$$\Psi_{\ell_2} : \{\mathbf{x} \in \mathbb{R}^2 | 0 \le x_1 \le 4, -4 \le x_2 \le 4\};$$

  The initial distribution Ω:
  $-x_1 \sim \mathcal{U}([-3.1, -0.9]),\ x_2 \sim \mathcal{U}([-0.6, 1.6]),$
  $-x_1 \sim \mathcal{N}(-2, 0.64), x_2 \sim \mathcal{N}(0.5, 0.32),$
  $-x_1 - 2.5 \sim \mathcal{E}(1),\ x_2 - 0.2 \sim \mathcal{E}(2),$
  $-\mathbf{x} \sim \mathit{Joint}\mathcal{N}_2\left(\begin{bmatrix} -2 \\ 0.5 \end{bmatrix}, \begin{bmatrix} 0.64 & 0.04 \\ 0.04 & 0.32 \end{bmatrix}\right);$
- The initial location: ℓ_1;
- The guard condition:

$$G_{\ell_1,\ell_2} : \{\mathbf{x} \in \mathbb{R}^2 : x_1^2 + x_2^2 \le 0.5625\},$$
$$G_{\ell_2,\ell_1} : \{\mathbf{x} \in \mathbb{R}^2 : x_1^2 + x_2^2 \le 0.25\};$$

- The reset:

$$R_{\ell_1,\ell_2} : x_1' = -x_1 \wedge x_2' = x_2,$$
$$R_{\ell_2,\ell_1} : x_1' = x_1 + 1 \wedge x_2' = x_2 + 1;$$

- The unsafe set:

$$X_u(\ell_1) : \{\mathbf{x} \in \mathbb{R}^2 : (x_1 + 1)^2 + (x_2 + 1)^2 \le 0.25\},$$
$$X_u(\ell_2) : \{\mathbf{x} \in \mathbb{R}^2 : (x_1 - 2)^2 + (x_2 - 2)^2 \le 0.25\}.$$

REFERENCES

[1] Alessandro Abate, Joost-Pieter Katoen, John Lygeros, and Maria Prandini. 2010. Approximate Model Checking of Stochastic Hybrid Systems. *European Journal of Control* 16, 6 (2010), 624–641.

[2] Matthias Althoff, Olaf Stursberg, and Martin Buss. 2008. Stochastic reachable sets of interacting traffic participants. In *Proc. of the IEEE Intelligent Vehicles Symposium*. IEEE, 1086–1092.

[3] Rajeev Alur, Costas Courcoubetis, Nicolas Halbwachs, Thomas A. Henzinger, P.-H. Ho, Xavier Nicollin, Alfredo Olivero, Joseph Sifakis, and Sergio Yovine. 1995. The algorithmic analysis of hybrid systems. *Theoretical computer science* 138, 1 (1995), 3–34.

[4] Michaël Bensimhoun. 2009. N-Dimensional Cumulative Function, And Other Useful Facts About Gaussians and Normal Densities. *Jerusalem, Israel, Tech. Rep* (2009).

[5] Olivier Bouissou, Alexandre Chapoutot, Adel Djaballah, and Michel Kieffer. 2014. Computation of parametric barrier functions for dynamical systems using interval analysis. In *Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on*. IEEE, 753–758.

[6] Manuela L. Bujorianu. 2004. Extended stochastic hybrid systems and their reachability problem. In *International Workshop on Hybrid Systems: Computation and Control*. Springer, 234–249.

[7] Manuela L. Bujorianu and John Lygeros. 2003. Reachability questions in piecewise deterministic Markov processes. In *International Workshop on Hybrid Systems: Computation and Control*. Springer, 126–140.

[8] Liyun Dai, Ting Gan, Bican Xia, and Naijun Zhan. 2017. Barrier Certificates Revisited. *Journal of Symbolic Computation* 80 (2017), 62–86.

[9] Thao Dang and Thomas Martin Gawlitza. 2011. *Discretizing Affine Hybrid Automata with Uncertainty*. Springer Berlin Heidelberg, 473–481.

[10] Thao Dang and Romain Testylier. 2012. Reachability Analysis for Polynomial Dynamical Systems Using the Bernstein Expansion. *Reliable Computing* 17, 2 (2012), 128–152.

[11] Christian Ellen, Sebastian Gerwinn, and Martin Fränzle. 2015. Statistical model checking for stochastic hybrid systems involving nondeterminism over continuous domains. *International Journal on Software Tools for Technology Transfer* 17, 4 (2015), 485–504.

[12] Martin Fränzle, Ernst Moritz Hahn, Holger Hermanns, Nicolás Wolovick, and Lijun Zhang. 2011. Measurability and Safety Verification for Stochastic Hybrid Systems. In *Proceedings of the 14th International Conference on Hybrid Systems: Computation and Control (HSCC'11)*. ACM, 43–52.

[13] William Glover and John Lygeros. 2004. A stochastic hybrid model for air traffic control simulation. *Proc. of the International Workshop on Hybrid Systems: Computation and Control* (2004), 372–386.

[14] Ernst Moritz Hahn, Arnd Hartmanns, Holger Hermanns, and Joost-Pieter Katoen. 2013. A compositional modelling and analysis framework for stochastic hybrid systems. *Formal Methods in System Design* 43, 2 (2013), 191–232.
[15] João Hespanha. 2004. Stochastic Hybrid Systems: Application to Communication Networks. *Proc. of the International Workshop on Hybrid Systems: Computation and Control* (2004), 47–56.
[16] João P. Hespanha. 2014. Modeling and analysis of networked control systems using stochastic hybrid systems. *Annual Reviews in Control* 38, 2 (2014), 155–170.
[17] Jianghai Hu, John Lygeros, and Shankar Sastry. 2000. Towards a theory of stochastic hybrid systems. In *International Workshop on Hybrid Systems: Computation and Control*. Springer, 160–173.
[18] A. Agung Julius. 2006. Approximate Abstraction of Stochastic Hybrid Automata. In *Proceedings of the International Workshop on Hybrid Systems: Computation and Control*. 318–332.
[19] James Kapinski, Jyotirmoy V. Deshmukh, Sriram Sankaranarayanan, and Nikos Aréchiga. 2014. Simulation-guided lyapunov analysis for hybrid dynamical systems. In *Proc. of the Hybrid Systems: Computation and Control (HSCC)*. ACM, 133–142.
[20] Hui Kong, Fei He, Xiaoyu Song, William N. N. Hung, and Ming Gu. 2013. Exponential-condition-based barrier certificate generation for safety verification of hybrid systems. In *Computer Aided Verification*. Springer, 242–257.
[21] Michal Kočvara and Michael Stingl. 2005. PENBMI User's guide (Version 2.0). (2005). Available at http://www.penopt.com.
[22] Marta Kwiatkowska, Gethin Norman, Jeremy Sproston, and Fuzhi Wang. 2004. Symbolic model checking for probabilistic timed automata. *Lecture notes in computer science* 3253 (2004), 293–308.
[23] Kim G. Larsen and Axel Legay. 2016. Statistical Model Checking: Past, Present, and Future. In *International Symposium on Leveraging Applications of Formal Methods*. Springer, 3–15.
[24] Axel LegayEmail and Mahesh Viswanathan. 2015. Statistical model checking: challenges and perspectives. *International Journal on Software Tools for Technology Transfer* 4 (2015), 369–376.
[25] André Platzer. 2011. Stochastic differential dynamic logic for stochastic hybrid programs. In *International Conference on Automated Deduction*. Springer, 446–460.
[26] Stephen Prajna and Ali Jadbabaie. 2004. Safety verification of hybrid systems using barrier certificates. In *International Workshop on Hybrid Systems: Computation and Control*. Springer, 477–492.
[27] Stephen Prajna, Ali Jadbabaie, and George J. Pappas. 2004. Stochastic safety verification using barrier certificates. In *Decision and Control, 2004. CDC. 43rd IEEE Conference on*, Vol. 1. IEEE, 929–934.
[28] Stephen Prajna, Ali Jadbabaie, and George J. Pappas. 2007. A framework for worst-case and stochastic safety verification using barrier certificates. *IEEE Trans. Automat. Control* 52, 8 (2007), 1415–1429.
[29] Stefan Ratschan and Zhikun She. 2007. Safety verification of hybrid systems by constraint propagation-based abstraction refinement. *ACM Transactions on Embedded Computing Systems* 6, 1 (2007), 573–589.
[30] Sriram Sankaranarayanan, Xin Chen, and Erika Abrahám. 2013. Lyapunov function synthesis using Handelman representations. In *The 9th IFAC Symposium on Nonlinear Control Systems*. 576–581.
[31] Mohamed Amin Ben Sassi, Romain Testylier, Thao Dang, and Antoine Girard. 2012. Reachability analysis of polynomial systems using linear programming relaxations. In *Automated Technology for Verification and Analysis*. Springer, 137–151.
[32] Fedor Shmarov and Paolo Zuliani. 2015. Probreach: verified probabilistic delta-reachability for stochastic hybrid systems. In *Proceedings of the 18th International Conference on Hybrid Systems: Computation and Control*. ACM, 134–139.
[33] Fedor Shmarov and Paolo Zuliani. 2016. Probabilistic Hybrid Systems Verification via SMT and Monte Carlo Techniques. In *Haifa Verification Conference*. Springer, 152–168.
[34] Andrew Sogokon, Khalil Ghorbal, Paul B. Jackson, and André Platzer. 2016. A Method for Invariant Generation for Polynomial Continuous Systems. In *Verification, Model Checking, and Abstract Interpretation*. Springer, 268–288.
[35] Jeremy Sproston. 2000. Decidable model checking of probabilistic hybrid automata. In *International Symposium on Formal Techniques in Real-Time and Fault-Tolerant Systems*. Springer, 31–45.
[36] Qinsi Wang, Paolo Zuliani, Soonho Kong, Sicun Gao, and Edmund M. Clarke. 2015. SReach: A Probabilistic Bounded Delta-Reachability Analyzer for Stochastic Hybrid Systems. In *Proceedings of the 13th International Conference on Computational Methods in Systems Biology CMSB 2015*. Springer, 15–27.
[37] Xia Zeng, Wang Lin, Zhengfeng Yang, Xin Chen, and Lilei Wang. 2016. Darboux-type barrier certificates for safety verification of nonlinear hybrid systems. In *Proceedings of the International Conference on Embedded Software (EMSOFT)*. IEEE, 1–10.
[38] Lijun Zhang, Zhikun She, Stefan Ratschan, Holger Hermanns, and Ernst Moritz Hahn. 2010. Safety verification for probabilistic hybrid systems. In *International Conference on Computer Aided Verification*. Springer, 196–211.

Received April 2017; revised May 2017; accepted June 2017