Scalable Long-term Safety Certificate for Large-scale Systems

Kenta Hoshino[1], Zhuoyuan Wang[2], Yorie Nakahira[2]

***Abstract*— This paper focuses on safe control problems for high-dimensional systems with large uncertainties. A major challenge is the computation burden required for long outlook horizons and large-scale systems. We approach this challenge using an integration of probabilistic reachability, the comparison theorem, PDE techniques, and probabilistic forward invariance. Specifically, we construct a probabilistic certificate for long-term safety that only requires myopically ensuring linear control constraints and evaluating two-dimensional PDEs regardless of the system dimension. The certificate is constructed by obtaining a long-term safe probability bound as a solution of the PDE using the comparison theorem and applying a new notion of probabilistic forward invariance on the probability bound. The use of probabilistic forward invariance on probabilistic reachability allows our method to carry the former's computation efficiency and the latter's control over long-term behaviors. Its capability to efficiently ensure long-term safety for high-dimensional systems can be useful in many large-scale distributed autonomous systems operating with limited onboard resources in latency-critical environments.**

I. Introduction

Making safe decisions under uncertainty is a key challenge for the safe deployment of many autonomous systems in the wild. Deterministic safe control methods have been well studied and can be used for systems with bounded/small disturbances [1], [2]. Some stochastic methods are designed to ensure the safety condition at each infinitesimal time intervals [3], [4], [5]. However, these methods may not guarantee long-term safety in stochastic systems because they cannot control the accumulation of risky tail probabilities, which is particularly problematic with large uncertainties. On the other hand, stochastic safe control approaches that account for longer time horizons (*e.g.,* stochastic barrier functions [6], probabilistic reachabilities [7], chance constrained predictive control [8]) either require heavy computation or give conservative actions to guarantee safety. There often have stringent tradeoffs between scalability, computation burden, fast response, over-conservatism, and long-term safety. Moreover, those tradeoffs are even more severe for high-dimensional systems.

There is a need for new methods that can ensure long-term safety in real time for systems operating with limited onboard resources in latency-critical environments. In this paper, we propose a scalable safety certificate and a control algorithm with guaranteed long-term safety. The proposed method reduces the computation burden of the following two processes: evaluation of long-term safe probability and generating control actions via optimizing long-term future. Below, we summarize our contributions and the features of the proposed method.

Scalable evaluation of long-term safe probability. Evaluation of long-term safe probability usually involves sampling the system trajectories or computing partial differential equations (PDEs) whose dimension scales with the size of the system. Such computation can be prohibitive for large-scale systems with limited onboard resources. Here, we first build upon the tools of [9] and comparison theorem of SDEs to show that the long-term safe probabilities can be lower bounded by the solution of two-dimensional PDEs regardless of the system dimension. This result enables highly compressed computation of the safety probability, thereby overcoming the curse of dimensionality in exhaustive Monte Carlo rollouts or solving high-dimensional PDEs.

Achieving long-term safety using myopic controllers. We propose a probabilistic certificate for long-term safety which can be used by a myopic controller or imposed as a linear constraint. This uses a novel notion of probabilistic forward invariance on the probability space proposed by [10]. This notion integrates probabilistic reachability and barrier function-based approaches and admits a generalization to unknown system parameters and multi-agent scenarios with limited communication [11], [12]. The integration of reachability- and invariance-based approaches will carry both the former's control over the long-term future and the latter's computation efficiency due to the use of myopic controllers.

The structure of this paper is as follows. Section II states the problem. Section III presents the proposed safety certificate and its theoretical guarantees. Section IV provides numerical examples. Section V concludes the paper.

Notations. Let $\mathbb{R}$ and $\mathbb{R}_+$ be the sets of real numbers and non-negative real numbers, respectively. Let $\mathbb{R}^n$ and $\mathbb{R}^{m\times n}$ be the n-dimensional Euclidean space and the space of $m\times n$ real matrices, respectively. To discuss stochastic systems, we denote a filtered probability space as the quadruple $(\Omega, \mathcal{F}, \mathbb{P}, \{\mathcal{F}_t\}_{t\in\mathbb{R}_+})$, where Ω is the sample space, $\mathcal{F}$ is the σ-field of Ω, $\mathbb{P}$ is the probability measure, and $\{\mathcal{F}_t\}_{t\in\mathbb{R}_+}$ is the filtration of $\mathcal{F}$. Throughout this paper, we assume that filtrations are right continuous and that $\mathcal{F}_0$ contains all the set of probability zero. Given the event $\mathcal{E}$, $\mathbb{P}(\mathcal{E})$ denotes the probability of $\mathcal{E}$, and $\mathbb{P}(\mathcal{E} \mid \mathcal{E}')$ denotes the conditional probability of $\mathcal{E}$ conditioned on the event $\mathcal{E}'$. For the random variable X, the notation $\mathbb{E}[X]$ represents the mathematical expectation of X. The conditional mathematical expectation

*This work is supported by JST, PRESTO Grant Number JPMJPR2136, ACT-X Grant Number JPMJAX210L, Japan.

[1]Kenta Hoshino is with the Department of Systems Science, Graduate School of Informatics, Kyoto University, Kyoto 606-8501, Japan, hoshino@i.kyoto-u.ac.jp.

[1]Zhuoyuan Wang and Yorie Nakahira are with the Department of Electrical and Computer Engineering, Carnegie Mellon Universty, {zhuoyuaw,ynakahir}@andrew.cmu.edu.

of X conditioned on the event $\mathcal{E}$ is denoted by $\mathbb{E}[X \mid \mathcal{E}]$. Given the event $\mathcal{E}$, the random variable Y, and the stochastic process X_t for $t \in \mathbb{R}_+$, $\mathbb{P}_x(\mathcal{E}) := \mathbb{P}(\mathcal{E} \mid X_0 = x)$ and $\mathbb{E}_x[Y] := \mathbb{E}[Y \mid X_0 = x]$, respectively.

II. Problem Statement

This section describes stochastic control systems in the subsection II-A and the goal of the safe control in the subsection II-B.

A. Description of Stochastic Control Systems

Here, we introduce the stochastic control systems considered throughout this paper. Let the control system be given by the Itô-type stochastic controlled differential equation

$$dX_t = (f(X_t) + g(X_t)U_t)\,dt + \sigma(X_t)dW_t,\ X_0 = x \quad (1)$$

where $X_t \in \mathbb{R}^n$ is the state, $U_t \in \mathbb{R}^m$ is the control, $W_t \in \mathbb{R}^\omega$ is the ω-dimensional standard Wiener process, $f : \mathbb{R}^n \to \mathbb{R}^n$, $g : \mathbb{R}^n \to \mathbb{R}^{n\times m}$, $\sigma : \mathbb{R}^n \to \mathbb{R}^{n\times\omega}$. To simplify the following discussion, we assume that the initial value $X_0 = x$ is deterministic.

We assume that the control policy is given by modifying a nominal controller to meet the safety specifications explained in the subsections II-B. Let the nominal controller be represented by

$$\hat{U}_t = N(X_t), \quad (2)$$

where $N : \mathbb{R}^n \to \mathbb{R}^m$. This controller is designed to satisfy operational goals, but may not necessarily guarantee safety. To ensure safety, the output of (2) will be certified or modified to produce the actual control action

$$U_t = K_N(X_t), \quad (3)$$

where $K_N : \mathbb{R}^n \to \mathbb{R}^m$.

Remark 1. We limit ourselves to Markov-type feedback control of (3), as opposed to control that depends on the past history of X_t. We demonstrate in section III that the myopic control design ensures long-term safety even for stochastic systems.

We denote the solution to the SDE (1) by X_t^N or $X_t^{K_N}$, expressing the dependence of the controllers N or K_N, or simply by X_t when no confusion arises.

Throughout the paper, we make the following assumptions.

Assumption 1. *The elements of $f(x)$, $g(x)$, $\sigma(x)$, $N(x)$, and $K_N(x)$ are locally Lipschitz continuous in x.*

Assumption 1 ensures the existence and uniqueness of the strong solution to the closed-loop system (1) with the controllers (2) and (3). See [13, Chapter IV] and [14, Chapter 5] for the definition and conditions for the strong solution of SDEs.

Assumption 2. *The solution X_t to the closed-loop system of (1) with the controllers (2) and (3) satisfies the non-explosion property, i.e., for the stopping time $\tau_\infty = \inf\{t \in \mathbb{R}_+ \mid X_t \notin \mathbb{R}^n\}$, $\mathbb{P}_x(\tau_\infty = \infty) = 1$ for any $x \in \mathbb{R}^n$.*

Assumption 2 implies that the solution of the closed-loop system X_t exists for any $t \in \mathbb{R}_+$ with probability one.

B. Safety specifications and design objectives

Recall from the previous section that the nominal controller aims to satisfy the operational goals but does not necessarily ensure safety. Here, our design objective is to ensure long-term safety by either certifying or modifying the output of the nominal controller. Let $\phi : \mathbb{R}^n \to \mathbb{R}$ be a barrier function, and

$$\mathcal{C}(L) := \{x \in \mathbb{R}^n : \phi(x) \geq L\} \quad (4)$$

be its L-superlevel set. The safe region in the state space is characterized by the zero superlevel set of the barrier function $\mathcal{C}(0)$.

The long-term safety is defined as: for any $t \in \mathbb{R}_+$ and for some $\epsilon \in (0, 1)$

$$\mathbb{E}_x\big[F(X_t^{K_N})\big] \geq 1 - \epsilon, \quad (5)$$

given the initial system state as $X_0 = x$, where $X_t^{K_N}$ is the solution to the system (1) with the controller (3) and $F(x)$ is given by

$$\begin{aligned} F(x) =& \mathbb{P}\left(X_\tau^N \in \mathcal{C}(0), \forall\tau \in [t, t+T] \mid X_t^N = x\right) \\ =& \mathbb{P}_x\left(\min_{0\leq t\leq T} \phi(X_t^N) \geq 0\right), \end{aligned} \quad (6)$$

with X_t^N be the solution to the SDE with the nominal controller $U_t = N(X_t)$ in (2). The second equality holds because the system (1) and (2) is time-invariant. The horizon length T is assumed to be $T > 0$. Because $0 \leq F(x) \leq 1$ for $x \in \mathbb{R}^n$, $\mathbb{E}_x[F(X_t^{K_N})]$ in (5) always satisfies $0 \leq \mathbb{E}_x[F(X_t^{K_N})] \leq 1$. Therefore, the parameter ϵ in (5) determines the tolerance level of the safety.

The condition (5) can be explained as follows. First, the function $F(x)$ of (6) is the probability that the state controlled by the nominal controller $U_t = N(X_t)$ stays within the safe set $\mathcal{C}(0)$ on the interval $[0, T]$ given the initial value $X_0 = x$. Then, $F(X_t^{K_N})$ in (5) is the probability that, given the state $X_t^{K_N}$, which is controlled by the safe controller (3) until time t, the state stays within $\mathcal{C}(0)$ on the horizon $[t, t+T]$ if the system is controlled by the nominal controller (2) on the future horizon. Accordingly, the value of $\mathbb{E}_x[F(X_t^{K_N})]$ gives the mathematical expectation of the safety probability $F(X_t^{K_N})$ at time t. The control design requires keeping the value of $\mathbb{E}_x[F(X_t^{K_N})]$ above $1 - \epsilon$. This control problem can be explained in a model predictive control-like fashion. We evaluate the future behavior of the system by using $F(X_t^{K_N})$ which expresses how safe the current state is when using the nominal controller on the future horizon. Then, we determine the control to keep the state within the safe set with a high probability depending on the value of $F(X_t^{K_N})$.

III. Proposed method and theoretical guarantees

In this section, we will first introduce our approach and preliminaries in section III-A, and then present the proposed

algorithm in section III-B, followed by the derivation of its theoretical properties in section III-C.

A. Probabilistic forward invariance

We introduce the operator $\mathcal{L}$ for a C^2 function $h : \mathbb{R}^n \to \mathbb{R}$ by

$$\mathcal{L}^U h(x) = L_f h(x) + L_g h(x) U + \frac{1}{2}\mathrm{Tr}\left(\frac{\partial^2 h}{\partial x^2}(x)\sigma(x)\sigma(x)^T\right), \tag{7}$$

where $L_f h$ and $L_g h$ are the Lie derivatives of the function h with f and g, respectively, and $\frac{\partial^2 h}{\partial x^2}$ is the Hessian of h.

Standard stochastic safe control methods for safe control consider forward invariance on the state space, and impose constraints on the control input to make the gradient of the barrier function point inwards the safe set. Mathematically, this is formulated as

$$\mathbb{P}(\mathcal{L}^{U_t}(\phi(X_t)) \geq 0 \mid X_t \in \partial\mathcal{C}) \geq 1 - \epsilon, \tag{8}$$

where X_t is the state of the system (1) at the time t, U_t is the control at the time t, and $\epsilon \in (0, 1)$ is the risk tolerance. This condition ensures safety of the system in the immediate next step with high probability, but will often lead to unsafe behaviour in the long run due to the accumulated error caused by the noises in the system.

In order to address this issue, [10] proposes to impose forward invariance on the probability space with the safety probability defined in (6). The control condition is

$$\mathcal{L}^{U_t} F(X_t) \geq -\alpha\left\{F(X_t) - (1-\epsilon)\right\}, \tag{9}$$

where F is given in (6), and $\alpha \geq 0$ is a tunable parameter. With this new condition, the long-term safety defined in (5) can be achieved. Furthermore, condition (9) is an affine constraint with respect to U_t, thus can be imposed as a linear constraint in convex problems. The evaluation $\mathcal{L}^{U_t} F(X_t)$ requires to evaluate the first and second derivatives of the probability $F(X_t)$ of (6). These quantities can be evaluated using Monte-Carlo simulation or numerically solving partial differential equations (PDEs). When Monte-Carlo simulation is used, the required number of sample system trajectories scales exponentially with the dimension of the system. When the PDE is used, one needs to solve a PDE whose dimension is at least the same as the dimension of the system, which is also intractable.

B. Proposed Safety Certificate and Control Algorithms

To address the issue mentioned above, we propose a modified safe control scheme. Instead of evaluating (9), we introduce a lower bound of $F(x)$ that can be evaluated by a PDE, which can be solved efficiently. The main machinery for obtaining the lower bound and the PDE is a comparison theorem for SDEs [15].

The proposed algorithm is outlined as follows. First, we consider the lower bound of $F(x)$. The definition of the function $F(x)$ in (6) shows $F(x)$ is the probability that the states X_t^N controlled by the nominal controller during the horizon of the length T will stay within the safe set. This is equivalent to the probability of $\phi(X_t^N)$ staying at non-negative values during the horizon. The comparison theorem of SDEs provides a kind of lower bound of $\phi(X_t^N)$, a scalar diffusion process ξ_t^{+-} given below. Due to its nature, the lower bound process ξ_t^{+-} can provide criteria to evaluate the probability of $\phi(X_t^N)$ staying non-negative during the horizon. A well-known result on stochastic processes allows us to evaluate the probability of the lower bound process ξ_t^{+-} keeping non-negative values throughout the horizon using a PDE concerning the scalar process ξ_t^{+-}. This probability provides the lower bound of $F(x)$. Then, we control a systems based on a condition for safe control using the lower bound of $F(x)$.

The lower bound of $F(x)$ is obtained as follows, using the comparison theorem of SDEs [15]. First, we introduce the functions $a : \mathbb{R}^n \to \mathbb{R}$ and $b : \mathbb{R}^n \to \mathbb{R}$ using the barrier function ϕ:

$$a(x) = \sum_{i,j,k} \sigma_k^i(x)\sigma_k^j(x)\frac{\partial\phi}{\partial x_i}(x)\frac{\partial\phi}{\partial x_j}, \quad b(x) = \frac{\mathcal{L}^N\phi(x)}{a(x)}, \tag{10}$$

where $\sigma_k^i(x)$ is the (i,k)-element of the diffusion coefficient $\sigma(x)$, and $\mathcal{L}^N$ is the operator $\mathcal{L}^U$ with $U = N(x)$. Additionally, let $\xi \in I \subset \mathbb{R}$ be a scalar variable, where I is the range of the barrier function $\phi(x)$. Using similar notations employed in [15], consider

$$a^+(\xi) = \sup_{x:\phi(x)=\xi} a(x), \quad b^-(\xi) = \inf_{x:\phi(x)=\xi} b(x). \tag{11}$$

Then, by using the functions a^+ and b^-, we introduce the following operator for a C^2 function $h : \mathbb{R} \to \mathbb{R}$:

$$\mathcal{L}^{+-}h(\xi) = a^+(\xi)\left\{\frac{1}{2}\frac{d^2h}{d\xi^2}(\xi) + b^-(\xi)\frac{dh}{d\xi}(\xi)\right\}. \tag{12}$$

As discussed later, this operator becomes the infinitesimal generator of a diffusion process ξ_t^{+-} that is a solution to the SDE

$$d\xi_t^{+-} = a^+(\xi_t^{+-})b^-(\xi_t^{+-})dt + \sqrt{a^+(\xi_t^{+-})}d\tilde{W}_t^+, \tag{13}$$

where $\tilde{W}_t^+$ is a one-dimensional standard Wiener process. We make the following assumption, which ensures the existence of a diffusion process ξ_t^{+-}.

Assumption 3. *The functions $\alpha^+(\xi)$ and $b^-(\xi)$ in (11) are globally Lipschitz continuous in $\xi \in I \subset \mathbb{R}$. Moreover, $a(x) > 0$ for any $x \in \mathbb{R}^n$.*

Next, we define the following function:

$$\underline{F}(\xi) = \mathbb{P}_\xi\left(\min_{0\leq t\leq T} \xi_t^{+-} \geq 0\right), \tag{14}$$

where ξ_t^{+-} is a scalar diffusion process given by the SDE (13) with $\xi_0^{+-} = \xi \in I \subset \mathbb{R}$. We set $\underline{F}(\xi) = 0$ for $\xi \leq 0$. Functions $F(x)$ and $\underline{F}(\xi)$ satisfy the following relation.

Lemma 1. *Assume that Assumptions 1, 2, and 3 hold. Then,*

$$\underline{F}(\phi(x)) \leq F(x), \ \forall x \in \mathbb{R}^n, \tag{15}$$

where $F(\cdot)$ and $\underline{F}(\cdot)$ are defined by (6) and (14), respectively.

Lemma 1 gives the lower bound of $F(x)$ in the design objective (5), and yields $\mathbb{E}_x[F(X_t^{K_N})] \geq \mathbb{E}_x[\underline{F}(\phi(X_t^{K_N}))]$. Therefore, this lower bound allows us to develop a control algorithm to achieve the design objective of (5).

The function $\underline{F}$ can be obtained by solving a 2-dimensional PDE. The probability in the right-hand side of (14) can be expressed as $\mathbb{P}_\xi(\min_{0\leq t\leq T} \xi_t^{+-} \geq 0) = \mathbb{P}_\xi(\tau^\xi > T)$, where $\tau^\xi = \inf\left\{t \in \mathbb{R}_+ \mid \xi_t^{+-} = 0\right\}$ is the first hitting time with $\xi_0^{+-} = \xi$. The well-known results on the probability distribution of the first hitting time [16] allows us to obtain the function $\underline{F}$ using a solution to the PDE given by

$$\frac{\partial u}{\partial t}(t,\xi) = \mathcal{L}^{+-}u(t,\xi) \text{ for } (t,\xi) \in (0,\infty) \times \mathring{I} \tag{16}$$

with the boundary conditions $u(0,\xi) = 1$ for $\xi \in \mathring{I}$ and $u(t,0) = 0$ for $t > 0$. The set $\mathring{I}$ is the interior of I. The solution of the PDE (16) gives $u(t,\xi) = \mathbb{P}(\tau^\xi > t)$, and accordingly we can obtain $\underline{F}(\xi) = u(T,\xi)$ where T is the safety time horizon in (6). The PDE (16) concerns the scalar space variable ξ, and thus is significantly easier to evaluate than the PDE in [17].

Using function $\underline{F}$, we show a sufficient condition for condition (5). To show the condition, define the function $\Lambda : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}$ by

$$\Lambda(x,U) = \mathcal{L}^U\left(\underline{F} \circ \phi\right)(x), \tag{17}$$

where the notation $\mathcal{L}^U\left(\underline{F} \circ \phi\right)$ means the operator $\mathcal{L}^U$ of (7) is applied for the composite function $\underline{F} \circ \phi(\cdot)$.

Theorem 1. *Let $\epsilon \in (0,1)$ and $\alpha \geq 0$. Assume that Assumptions 1, 2, 3 hold. Moreover, assume that the function $\underline{F}(\xi)$ is twice continuously differentiable at $\xi = 0$. Further, assume that the initial value $X_0 = x_0$ of the system (1) satisfies $\underline{F}(\phi(x_0)) \geq 1-\epsilon$. If for any $x \in \mathbb{R}^n$, the controller K_N satisfies*

$$\Lambda(x, K_N(x)) \geq -\alpha\left\{\underline{F}(\phi(x)) - (1-\epsilon)\right\}, \tag{18}$$

then the closed-loop system (1) and (3) satisfy the condition (5).

From Theorem 1, to achieve the safety specification (5), it suffices finding a control satisfying the condition (18). Such control action can be solved efficiently because (18) is a linear constraint of the control action U. Thus, it can be integrated into the following quadratic program. At each time t, the system observes X_t and solves

$$\begin{aligned} &\min_U \|U - N(X_t)\|^2 \\ &\text{s.t. } \Lambda(X_t,U) \geq -\alpha\left\{\underline{F}(\phi(X_t)) - (1-\epsilon)\right\}. \end{aligned} \tag{QP}$$

As stated in subsection II-A, we obtain the safe controller K_N from the nominal controller $N(x)$. Given the solution $U^*(x)$ of (QP), the controller is given by $K_N(x) = U^*(x)$. The local Lipschitz continuity of $K_N(x)$ obtained by (QP) can be shown by adapting Theorem 3 of [18].

The above algorithm is summarized in Algorithm 1.

Algorithm 1 Safe control algorithm

```
Define Δt, T
Solve PDE (16); F(ξ) ← u(T, ξ).
t ← 0
while t < T_end do
    Observe X_t
    Solve (QP) to obtain K_N(X_t) = U*(X_t)
    Execute control U_t = K_N(X_t)
    t ← t + Δt
end while
```

C. Derivation of theoretical guarantees

We here show the proofs of Lemma 1 and Theorem 1. To prove them, we first show that $\mathcal{L}^{+-}$ gives a diffusion process ξ_t^{+-}.

Lemma 2. *Assume that Assumption 3 holds. Then, there exists a diffusion process ξ_t^{+-} whose generator is $\mathcal{L}^{+-}$. In other words, ξ_t^{+-} is a weak solution to the SDE (13) with the initial value $\xi_0^{+-} = \xi_0 \in I$.*

Proof. It is straightforward to see that the SDE (13) possesses the generator $\mathcal{L}^{+-}$. Conversely, according to the continuity of the coefficients in Assumption 3 and the existence results on the martingale problem [13, Chapter IV], the generator ensures the existence of the diffusion process ξ_t^{+-} that follows the SDE (13). ■

We give the proof of Lemma 1.

Proof of Lemma 1. Applying the Itô formula to $\phi(X_t)$, we obtain

$$d\phi(X_t) = \mathcal{L}^{U_t}\phi(X_t)dt + \frac{\partial \phi}{\partial x}(X_t)\sigma(X_t)dW_t. \tag{19}$$

Note that the SDE (13) is a modification of the SDE (19) using the functions $a^+(\xi)$ and $b^-(\xi)$. From [15, Theorem 3.1], there exists a probability space such that the following conditions hold.

1) There exits a stochastic process ξ_t that has the same law as that of $\phi(X_t)$.
2) The inequality
$$\min_{0\leq s\leq t} \xi_s^{+-} \leq \min_{0\leq s\leq t} \xi_s \tag{20}$$
holds with probability one for any $t \in \mathbb{R}_+$ when $\xi_0^{+-} = \xi_0$.

Condition 1 implies that

$$\mathbb{P}_{\xi_0}\left(\min_{0\leq s\leq t} \xi_s \geq 0\right) = \mathbb{P}_{X_0}\left(\min_{0\leq s\leq t} \phi(X_s) \geq 0\right) \tag{21}$$

holds when $\xi_0 = \phi(X_0)$. Condition 2 implies that

$$\mathbb{P}_{\xi_0}\left(\min_{0\leq s\leq t} \xi_s^{+-} \geq 0\right) \leq \mathbb{P}_{\xi_0}\left(\min_{0\leq s\leq t} \xi_s \geq 0\right) \tag{22}$$

holds. Therefore, replacing ξ_0 and X_0 with $\phi(x)$ and x, respectively, the inequality (22) implies the inequality (15), which completes the proof. ■

Remark 2. Intuitively, the process ξ_t can be regarded as $\phi(X_t)$. However, due to the limitation of the comparison theorem [15], we cannot argue pathwise statements such as $\min_{0\le s\le t}\xi_s^{+-} \le \min_{0\le s\le t}\phi(X_s)$. Instead, we compare the probabilities of events on ξ_t^{+-} and $\phi(X_t)$ by combining (21) and (22).

Finally, we prove Theorem 1.

Proof of Theorem 1. Lemma 2 implies the existence of the solution ξ_t^{+-} to the SDE (13). Lemma 1 guarantees $\underline{F}(\phi(x)) \le F(x)$ for $x \in \mathbb{R}^n$. Taking conditional expectation on both sides yields

$$\mathbb{E}_x\left[F(X_t^{K_N})\right] \ge \mathbb{E}_x\left[\underline{F}(\phi(X_t^{K_N}))\right]. \tag{23}$$

Additionally, the function $\underline{F}(\cdot)$ is given as a solution to the PDE (16). Under Assumption 3, we can show that the PDE (16) admits a weak solution $u(t,\xi)$ such that $u(t,\xi)$ is twice continuously differentiable for any $\xi \in \mathring{I}$ when $t > 0$ [16, Proposition 6]. Because $\underline{F}(\xi)$ is given by $\underline{F}(\xi) = u(T,\xi)$, $\underline{F}(\xi)$ is a C^2 function on $\mathring{I}$. Under the assumption of the twice differentiability of $\underline{F}(\xi)$ at $\xi = 0$, $\mathcal{L}^{K_N}(\underline{F}\circ\phi)(x)$ is well defined for $x \in \mathbb{R}^n$. Dynkin's formula implies

$$\frac{d}{dt}\mathbb{E}_x[\underline{F}(\phi(X_t^{K_N}))] = \mathbb{E}_x\left[\mathcal{L}^{K_N}\left(\underline{F}\circ\phi\right)(X_t^{K_N})\right]. \tag{24}$$

Condition (18) implies

$$\frac{d}{dt}\mathbb{E}_x[\underline{F}(\phi(X_t^{K_N}))] \ge -\alpha\left\{\mathbb{E}_x[\underline{F}(\phi(X_t^{K_N}))] - (1-\epsilon)\right\}. \tag{25}$$

The ordinary differential equation

$$\dot{w}(t) = -\alpha\left(w(t) - (1-\epsilon)\right) \tag{26}$$

possesses the solution

$$w(t) = (1-\epsilon) + (w(0) - (1-\epsilon))e^{-\alpha t}. \tag{27}$$

Note that when $w(0)$ is given by $w(0) = \underline{F}(\phi(x)) \ge 1-\epsilon$,

$$w(t) \ge 1-\epsilon \quad \forall t \ge 0, \tag{28}$$

for any $\alpha \ge 0$. The standard differential inequality result, such as [19, Chapter I, Theorem 6.1], implies that

$$\mathbb{E}_x[\underline{F}(\phi(X_t^{K_N}))] \ge w(t) \ge 1-\epsilon, \quad \forall t \ge 0. \tag{29}$$

This completes the proof. ■

IV. Numerical Example

We demonstrate the safe control using the proposed control design condition. The proposed control method enables a scalable control design for the safety control problem for high-dimensional systems, which is challenging in the previous study [10].

We test the proposed method using noisy n-th order integrator

$$dX_t^{(i)} = X_t^{(i+1)}dt,\ dX_t^{(n)} = U_t dt + \sigma dW_t, \tag{30}$$

where $1 \le i \le n-1$, $X_t = (X_t^{(1)},\dots,X_t^{(n)})^T \in \mathbb{R}^n$ is the state, $U_t \in \mathbb{R}$ is the control input, W_t is the scalar standard Wiener process, and $\sigma \in \mathbb{R}_+$. The nominal controller is given by

$$N(X_t) = -k_1 r\tanh(X_t^{(1)}/r) - \sum_{i=2}^{n} k_i X_t^{(i)}, \tag{31}$$

where $k_i \in \mathbb{R}$ $(i = 1,\dots,n)$ are the gain parameters, and r is a sufficiently large positive parameter. This nominal controller is a modification of a stabilizing feedback controller for the integrator. Therefore, when the initial value is close to the origin, the system state tends to converge to the origin. The safe set is given by $\mathcal{C}(0) = \{x : \phi(x) \ge 0\}$ with the barrier function $\phi(x) = c^T x + d$, where $c \in \mathbb{R}^n$, $x \in \mathbb{R}^n$, and $d \in \mathbb{R}$.

We show the results of the numerical experiment when $n = 10$ with parameters $\sigma = 1$, $d = 3$, $r = 10$, $\epsilon = 0.1$, $\alpha = 2$. We use pole placement to design the nominal feedback control k with poles $p = -[0.4, 0.5, \cdots, 1.3]$, and we let $c = [k_2, k_3, \cdots, k_{10}, 1]$. Then, the functions $a^+(\xi)$ and $b^-(\xi)$ in (10) becomes $a^+(\xi) = 1$ and $b^-(\xi) = -r = -10$, respectively. We apply the proposed control algorithm in Algorithm 1 to the system (30). We set the initial value of the state as $X_0 = (0.5, \cdots, 0.5)^T$.

We compare the control results of the proposed safe control strategy with the nominal controller (31). Fig. 1 shows the barrier function value for systems with and without the safe control. It can be seen that with the proposed safe control, the barrier function value of the high dimensional system will remain positive during the experiment time, whereas the nominal control will yield negative barrier function value, indicating unsafe behaviours. Fig. 2 shows the empirical probabilities by calculating the ratio of safe trajectories over all the trajectories. Long-term safety is ensured with the proposed control, while the safety probability keeps decreasing over time for the nominal control. Fig. 3 visualizes the sample trajectories of system (30) with $n = 2$. We set $X_0 = [2,3]^T, k = [1,1]^T$ for better visualizations, and other settings remain the same. We can see that without the safe control, a large portion of the trajectories violate the safety boundary. On the contrary, the safe control can successfully maintain the system states in the safe region with high probability.

To investigate the computation efficiency of the proposed method, we conducted the numerical simulation for systems from $n = 2$ to $n = 4$ and report their computation times. The simulations require solving the PDE (16), solving the SDE (30), and determining the safe control by solving the QP. We solved the SDE (30) for $t \in [0, 10]$ using the Euler-Maruyama method with time step $\Delta t = 0.01$. We use standard finite-difference method to solve the PDE (16). Table I shows the mean and standard deviation of the computation times in the total simulations for a sample trajectory, the computation times for solving the PDE (16), and the mean of the computation time of QP for the control in each time step, for $n = 2, 3, 4$. The computation times for numerically solving the PDE (16) do not vary much with the dimension n because the space dimension of the PDE is

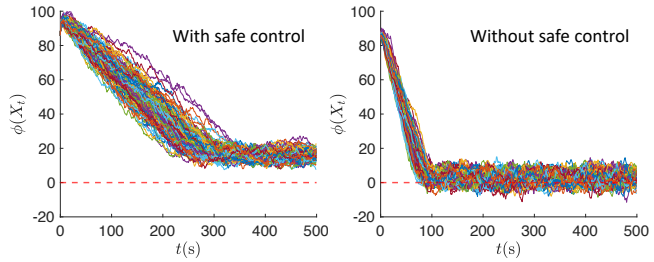

Fig. 1: Barrier function values for the 10-dimensional system with (left) and without (right) safe control.

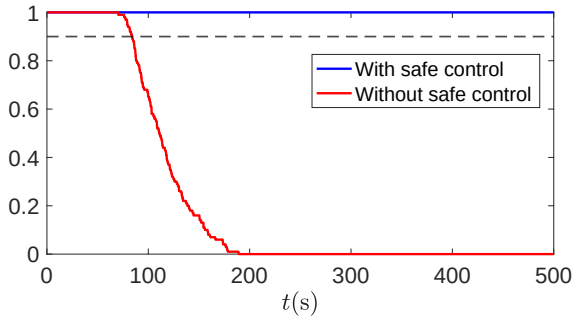

Fig. 2: Empirical safety probability for the 10-dimensional system with and without safe control.

always scalar. The computation times for solving QP are also sufficiently small, thus enables scalable and computationally feasible safe control in real time.

TABLE I: Computation times

	$n=2$	$n=3$	$n=4$
Total time [s]	2.44 ± 0.20	3.22 ± 0.12	3.08 ± 0.16
PDE (16) [s]	0.78	1.71	1.48
QP per time step [s]	2.0×10^{-6}	2.0×10^{-6}	2.0×10^{-6}

V. Conclusion

In this paper, we present a computationally efficient safe control method using a combination of probabilistic reachability, the comparison theorem, PDE techniques, and probabilistic forward invariance. The proposed method has the following features: scalability in the evaluation of long-term safe probability, and assurance of long-term safety using myopic controllers.

References

[1] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, "Control barrier functions: Theory and applications," in *2019 18th European Control Conference (ECC)*. IEEE, 2019, pp. 3420–3431.

[2] S. Bansal, M. Chen, S. Herbert, and C. J. Tomlin, "Hamilton-jacobi reachability: A brief overview and recent advances," in *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*. IEEE, 2017, pp. 2242–2253.

[3] A. Clark, "Control barrier functions for complete and incomplete information stochastic systems," in *2019 American Control Conference (ACC)*. IEEE, 2019, pp. 2928–2935.

[4] M. Ahmadi, X. Xiong, and A. D. Ames, "Risk-sensitive path planning via cvar barrier functions: Application to bipedal locomotion," *arXiv preprint arXiv:2011.01578*, 2020.

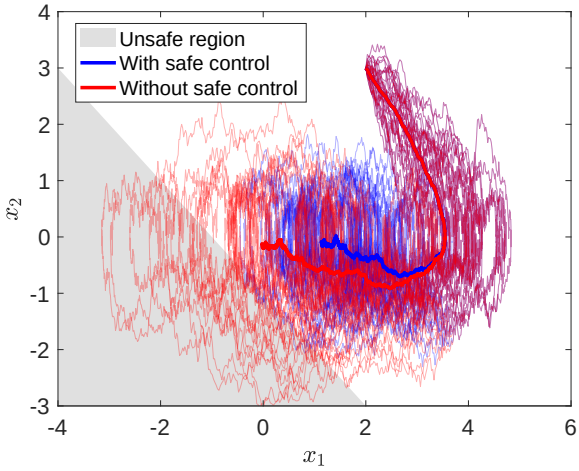

Fig. 3: State trajectories of the 2-dimensional system with and without safe control. Bold lines show the averaged trajectories.

[5] W. Luo, W. Sun, and A. Kapoor, "Multi-robot collision avoidance under uncertainty with probabilistic safety barrier certificates," *Advances in Neural Information Processing Systems*, vol. 33, pp. 372–383, 2020.

[6] C. Wang, Y. Meng, S. L. Smith, and J. Liu, "Safety-critical control of stochastic systems using stochastic control barrier functions," in *2021 60th IEEE Conference on Decision and Control (CDC)*. IEEE, 2021, pp. 5924–5931.

[7] A. Abate, S. Amin, M. Prandini, J. Lygeros, and S. Sastry, "Probabilistic reachability and safe sets computation for discrete time stochastic hybrid systems," in *Proceedings of the 45th IEEE Conference on Decision and Control*. IEEE, 2006, pp. 258–263.

[8] A. T. Schwarm and M. Nikolaou, "Chance-constrained model predictive control," *AIChE Journal*, vol. 45, no. 8, pp. 1743–1752, 1999.

[9] K. Hoshino, "On estimate of settling-time distributions of finite-time stable stochastic systems," in *2022 61th IEEE Conference on Decision and Control (CDC)*, 2022, accepted.

[10] Z. Wang, H. Jing, C. Kurniawan, A. Chern, and Y. Nakahira, "Myopically verifiable probabilistic certificate for long-term safety," *arXiv preprint arXiv:2110.13380*, 2021.

[11] S. Gangadhar, Z. Wang, H. Jing, and Y. Nakahira, "Adaptive safe control for driving in uncertain environments," in *2022 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, 2022, pp. 1662–1668.

[12] H. Jing and Y. Nakahira, "Probabilistic safety certificate for multi-agent systems," in *2022 61th IEEE Conference on Decision and Control (CDC)*, 2022, accepted.

[13] N. Ikeda and S. Watanabe, *Stochastic differential equations and diffusion processes*. Elsevier, 2014.

[14] I. Karatzas and S. Shreve, *Brownian motion and stochastic calculus*. springer, 2014, vol. 113.

[15] N. Ikeda and S. Watanabe, "A comparison theorem for solutions of stochastic differential equations and its applications," *Osaka Journal of Mathematics*, vol. 14, no. 3, pp. 619–633, 1977.

[16] P. Patie and C. Winter, "First exit time probability for multidimensional diffusions: A PDE-based approach," *Journal of computational and applied mathematics*, vol. 222, no. 1, pp. 42–53, 2008.

[17] A. Chern, X. Wang, A. Iyer, and Y. Nakahira, "Safe control in the presence of stochastic uncertainties," in *2021 60th IEEE Conference on Decision and Control (CDC)*, pp. 6640–6645.

[18] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs for safety critical systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 8, pp. 3861–3876, 2016.

[19] J. Hale, *Ordinary Differential Equations*. Dover Publications, 2009.