Safety Verification of Stochastic Systems: A Set-Erosion Approach

Zishun Liu, Saber Jafarpour, *Member, IEEE*, and Yongxin Chen, *Senior Member, IEEE*

***Abstract*—We study the safety verification problem for discrete-time stochastic systems. We propose an approach for safety verification termed set-erosion strategy that verifies the safety of a stochastic system on a safe set through the safety of its associated deterministic system on an eroded subset. The amount of erosion is captured by the probabilistic bound on the distance between stochastic trajectories and their associated deterministic counterpart. Building on recent development of stochastic analysis, we establish a sharp probabilistic bound on this distance. Combining this bound with the set-erosion strategy, we establish a general framework for the safety verification of stochastic systems. Our method is versatile and can work effectively with any deterministic safety verification techniques. We exemplify our method by incorporating barrier functions designed for deterministic safety verification, obtaining barrier certificates much tighter than existing results. Numerical experiments are conducted to demonstrate the efficacy and superiority of our method.**

***Index Terms*—Stochastic system, nonlinear system, safety verification.**

I. Introduction

SAFETY is a fundamental requirement for a wide range of real-world systems, including autonomous vehicles, robots, power grids, and beyond. Motivated by the significance of safety, research on safety verification has flourished in recent decades. Typically, safety verification refers to the process of verifying whether the system state remains within a defined safe region over a specified time horizon, whether in discrete-time or continuous-time contexts [2]. In this letter, we focus on the safety verification problem for discrete-time systems.

Since the safety of real-world systems is frequently challenged by uncertainties in the environment [3], it is essential for safety verification schemes to account for disturbances. Most existing approaches have modeled disturbances as bounded deterministic inputs and verified the safety in the worst case through deterministic methods such as dynamic programming [4], [5], barrier certification [6] and ISSf-barrier functions [7]. Among these deterministic methods, barrier certification has attracted growing attention thanks to its simplicity and has been widely adopted to formally prove the safety of nonlinear and hybrid systems [8].

Many real-world applications are subject to stochastic disturbances [9]. In such cases, traditional deterministic methods often become either inapplicable or overly conservative, as they focus on worst-case scenarios that rarely happen [10]. To better reflect the effects of stochastic disturbances, stochastic safety verification shifts the focus to ensuring safety within a safe set with high probability, e.g., a finite-time stochastic trajectory stays in the safe set with probability $> 99.9\%$.

Multiple techniques have been developed for the safety verification of discrete-time stochastic systems. For instance, martingale-based strategies [10], [11], [12] focus on constructing barrier functions that utilize semi-martingale or c-martingale conditions [13] to bound the failure probability. Another commonly used method is direct risk estimation [14], [15], [16], which first bounds the failure probability of the system state at a single time instance, then applies a union bound over the entire time horizon. Some other methods such as conformal prediction [17] and optimization-based approaches with chance constraints [18] are also applied in practice. However, all these techniques are often either overly conservative for ensuring safety with high probability or limited to specific, restrictive scenarios.

In this letter, we present a novel approach termed *set-erosion* strategy for verifying the safety of discrete-time stochastic systems. Our strategy states that to verify the safety of a stochastic system on a set with a certain probabilistic guarantee, it suffices to verify the safety of its associated deterministic system on an eroded subset. The degree of erosion is quantified by the probabilistic bound on the distance between stochastic trajectories and their deterministic counterparts, termed stochastic trajectory gap. We provide a sharp probabilistic bound for this gap, enabling the set-erosion strategy to effectively reduce the stochastic safety verification problem to a deterministic one. This framework is compatible with various deterministic safety verification approaches, including barrier certification discussed in this letter. Although some existing methods such as [19], [20] are motivated by a similar intuition with set erosion, our derived bound is significantly tighter than existing methods when the

Received 13 September 2024; revised 18 November 2024; accepted 10 December 2024. Date of publication 16 December 2024; date of current version 24 December 2024. This work was supported by NSF under Grant 1942523, Grant 2206576, and Grant 2409016. Recommended by Senior Editor S. Dey. *(Corresponding author: Yongxin Chen.)*

Zishun Liu and Yongxin Chen are with the School of Aerospace Engineering, Georgia Institute of Technology, Atlanta, GA 30332 USA (e-mail: zliu910@gatech.edu; yongchen@gatech.edu).

Saber Jafarpour is with the Electrical, Computer, and Energy Engineering Department, University of Colorado Boulder, Boulder, CO 80309 USA (e-mail: Saber.Jafarpour@colorado.edu).

Digital Object Identifier 10.1109/LCSYS.2024.3518394

probabilistic guarantee is high and the time horizon is long. Consequently, our method gives a notably less conservative safety verification result in safety-critical applications for stochastic systems.

Notations: The set of positive integers is denoted by $\mathbb{N}_+$. We use $\|\cdot\|$ to denote ℓ_2 norm. Given two sets $A, B \subseteq \mathbb{R}^n$, the Minkowski sum of them is defined by $A \oplus B = \{x + y : x \in A,\ y \in B\}$, and the Minkowski difference is defined by $A \ominus B = (A^c \oplus (-B))^c$, where A^c, B^c are the complements of A, B and $-B = \{-y : y \in B\}$. We use $\mathbb{E}$ to denote expectation, $\mathbb{P}$ to denote probability, $\mathcal{N}(\mu, \Sigma)$ to denote Gaussian distribution, $\mathcal{B}^n(r, y)$ to denote the ball $\{x \in \mathbb{R}^n : \|x - y\| \leq r\}$, and $\mathcal{S}^{n-1}$ to denote the unit sphere $\{x \in \mathbb{R}^n : \|x\| = 1\}$. For a random variable X, $X \sim G$ means X is independent and identically drawn from the distribution G. We say $\alpha(\cdot) : \mathbb{R} \to \mathbb{R}$ is an extended class $\mathcal{K}$ function if $\alpha(0) = 0$ and $\alpha(\cdot)$ is increasing on $\mathbb{R}$.

II. Problem Statement

Consider the discrete-time stochastic system

$$X_{t+1} = f(X_t, d_t, t) + w_t, \tag{1}$$

where $X_t \in \mathbb{R}^n$ is the system state, $d_t \in \mathcal{D} \subset \mathbb{R}^m$ is a bounded disturbance whose statistical properties cannot be captured, $w_t \in \mathbb{R}^n$ is the stochastic disturbance and $f : \mathbb{R}^n \times \mathbb{R}^m \times \mathbb{N}_+ \to \mathbb{R}^n$ is a smooth transition function. In this letter, we impose the Lipschitz nonlinearity condition on the system.

Assumption 1: At every time $t \geq 0$, there exists $L_t \geq 0$ such that $\|f(x, d, t) - f(y, d, t)\| \leq L_t \|x - y\|$ holds for every $x, y \in \mathbb{R}^n$ and every $d \in \mathcal{D} \subset \mathbb{R}^m$.

We model w_t as *sub-Gaussian* disturbance, which includes a wide range of noise distributions such as Gaussian, uniform, and any zero-mean distributions with bounded support [21, Sec. 2].

Definition 1 (Sub-Gaussian): A random variable $X \in \mathbb{R}^n$ is said to be sub-Gaussian with variance proxy σ^2, denoted as $X \sim subG(\sigma^2)$, if $\mathbb{E}(X) = 0$ and $\mathbb{E}_X(e^{\lambda\langle \ell, X\rangle}) \leq e^{\frac{\lambda^2\sigma^2}{2}}$ holds for all $\lambda \in \mathbb{R}$ and $\ell \in \mathcal{S}^{n-1}$.

Assumption 2: For the discrete-time stochastic system (1), $w_t \sim subG(\sigma_t^2)$ with some finite $\sigma_t > 0$, $\forall t \geq 0$.

This letter aims to establish an effective safety verification method for the stochastic system (1). To formulate this problem, we first formalize the concept of safety for the deterministic systems [8]. Consider the deterministic system

$$x_{t+1} = f(x_t, d_t, t), \tag{2}$$

which can be treated as the stochastic-noise-free version of the stochastic system (1). Given a terminal time $T \in \mathbb{N}_+$ and a safe set $\mathcal{C} \subseteq \mathbb{R}^n$, we say the deterministic system (2) starting from $\mathcal{X}_0$ is *safe* during $t \leq T$ if $\mathcal{X}_0 \subseteq \mathcal{C}$ and

$$x_0 \in \mathcal{X}_0 \ \Rightarrow\ x_t \in \mathcal{C}, \qquad \forall t \leq T,\ \forall d_t \in \mathcal{D}. \tag{3}$$

For the stochastic system (1), safety in the sense of (3) can be restrictive. When w_t is unbounded, X_t is likely to be unbounded, thus any bounded set in $\mathbb{R}^n$ will be judged as unsafe. Even if w_t is bounded, (3) completely ignores the statistical property of the stochastic noise and requires the state to stay in $\mathcal{C}$ to the worst case of w_t, which rarely happens due to the stochastic nature of the noise. This usually leads to conservative safety guarantees. For these reasons, we focus on safety with probabilistic guarantee to better capture the effect of the stochastic noise.

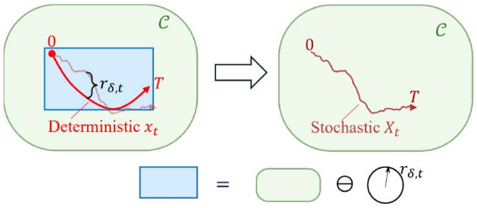

Fig. 1. An illustration of set-erosion strategy. Here $\mathcal{C}$ in green is the safe set, and the blue area is the eroded subset $\mathcal{C} \ominus \mathcal{B}^n(r_{\delta,t}, 0)$ with $r_{\delta,t}$ given in Theorem 1-2). By Theorem 1, if the deterministic trajectory stays in the blue area at any time, then the stochastic trajectory is safe on $\mathcal{C}$ with $1 - \delta$ guarantee.

Definition 2: Consider the stochastic system (1) with the bounded set $\mathcal{D} \subseteq \mathbb{R}^m$. Given a $\delta \in [0, 1]$, a safe set $\mathcal{C} \subset \mathbb{R}^n$, an initial configuration $\mathcal{X}_0 \subseteq \mathbb{R}^n$ and a terminal time T, the system is said to be *safe with* $1 - \delta$ *guarantee* during $t \leq T$ if $\mathcal{X}_0 \subseteq \mathcal{C}$ and:

$$X_0 \in \mathcal{X}_0 \ \Rightarrow\ \mathbb{P}(X_t \in \mathcal{C},\ \forall t \leq T) \geq 1 - \delta. \tag{4}$$

With this definition, the stochastic safety verification problem we seek to solve can be formalized below.

Problem 1 (Stochastic Safety Verification): Consider a stochastic system (1) under Assumptions 1 and 2. Develop an effective strategy to verify its safety with $1 - \delta$ guarantee during a finite horizon $t \leq T$.

III. Set-Erosion Strategy

Intuitively, the stochastic system (1) is fluctuating around its associated deterministic system (2) with high probability. Given a safe set $\mathcal{C} \subset \mathbb{R}^n$, if we erode/shrink $\mathcal{C}$ from its boundary to get a subset $\tilde{\mathcal{C}} \subset \mathcal{C}$, which is separated from the "robustness buffer" $\mathcal{C} \backslash \tilde{\mathcal{C}}$, and verify that the deterministic system (2) is safe on $\tilde{\mathcal{C}}$, then the fluctuation of the stochastic trajectories would probably stay in the robustness buffer and not exceed $\mathcal{C}$. Building on this intuition, we propose a strategy termed *set-erosion* for stochastic safety verification. This strategy can be viewed as the dual to the separation strategy for stochastic reachability analysis proposed in [22].

For the associated systems (1) and (2), we say X_t and x_t are *associated* trajectories if they have the same initial state $X_0 = x_0$ and the same d_t at any time. The fluctuation of the stochastic system (1) around the deterministic system (2) can be quantified by the distances among pairs of associated trajectories. The set-erosion strategy produces a sufficient condition for the safety of the stochastic system (1) with $1 - \delta$ guarantee, as formalized below.

Theorem 1 (Set-Erosion Strategy): Consider the stochastic system (1) and its associated deterministic system (2). Given a safe set $\mathcal{C} \in \mathbb{R}^n$, an initial set $\mathcal{X}_0 \in \mathcal{C}$, and a terminal time T, if there exists $r_{\delta,t} : \mathbb{N}_+ \to \mathbb{R}_+$ such that for any trajectory X_t of (1) and its associated trajectory x_t of (2) starting from $\mathcal{X}_0$:

1) $\mathbb{P}\big(\|X_t - x_t\| \leq r_{\delta,t},\ \forall\ t \leq T\big) \geq 1 - \delta$,

2) $x_t \in \mathcal{C} \ominus \mathcal{B}^n(r_{\delta,t}, 0)$, for all $t \leq T$,

then the system (1) is safe with $1 - \delta$ guarantee during $t \leq T$.

Proof: Let X_t be any trajectory of (1) associated with a trajectory x_t of (2). Then, by Condition 1 and the definition of the Minkowski sum,

$$\mathbb{P}\big(X_t \in \{x_t\} \oplus \mathcal{B}^n(r_{\delta,t}, 0), \forall t \leq T\big) \geq 1 - \delta.$$

By Condition 2, $\mathbb{P}(X_t \in \mathcal{C}, \forall t \leq T) \geq 1 - \delta$ follows. ■

An illustration of Theorem 1 is shown in Figure 1. We term $r_{\delta,t}$ in Theorem 1 as the probabilistic bound on *stochastic trajectory gap*, as it represents the gap between stochastic trajectories and their deterministic counterpart over a time horizon. It quantifies the *erosion depth* in the Minkowski difference $\mathcal{C} \ominus \mathcal{B}^n(r_{\delta,t}, 0)$. Theorem 1 states that once a probabilistic bound $r_{\delta,t}$ of the stochastic trajectory gap is provided, then to verify the safety of the stochastic system on $\mathcal{C}$, it suffices to verify the safety of its *associated deterministic system* on the eroded subset $\mathcal{C} \ominus \mathcal{B}^n(r_{\delta,t}, 0)$.

The effectiveness of the set-erosion strategy relies on the tightness of $r_{\delta,t}$. If $r_{\delta,t}$ is too large, then $\mathcal{C} \ominus \mathcal{B}^n(r_{\delta,t}, 0)$ can be very small or even empty, rendering conservative conditions. Therefore, it is crucial to establish a tight probabilistic bound $r_{\delta,t}$ for the stochastic trajectory gap.

IV. Probabilistic Bound on Stochastic Trajectory Gap

In this section, we present two approaches to probabilistically bounding the stochastic trajectory gap. The first one is based on a novel stochastic analysis technique developed in our previous work [1]. The second one follows the idea of worst-case analysis and is presented for comparison. By comparing the two, we demonstrate that the former is always superior to the latter.

A. Probabilistic Bound Based on Stochastic Deviation

In [1], we introduce the notion of *stochastic deviation* as the distance $\|X_t - x_t\|$ between associated X_t and x_t at a single time t, and give a tight probabilistic bound on the stochastic deviation. This bound is established by leveraging a novel function called the Averaged Moment Generating Function and the Markov inequality. We refer to our recent works [1], [22] for more details.

Proposition 1 (Stochastic Deviation [1]): Consider the stochastic system (1) and its associated deterministic system (2) under Assumptions 1 and 2. Let X_t be the trajectory of (1) and x_t be the associated trajectory of (2). Then, given $t \geq 0$, for any $\delta \in (0, 1)$ and tunable parameter $\varepsilon \in (0, 1)$,

$$\|X_t - x_t\| \leq \sqrt{\Psi_t(\varepsilon_1 n + \varepsilon_2 \log(1/\delta))} \tag{5}$$

holds with probability at least $1 - \delta$, where

$$\Psi_t = \psi_{t-1} \sum_{k=0}^{t-1} \sigma_k^2 \psi_k^{-1}, \quad \psi_t = \prod_{k=0}^{t} L_k^2, \tag{6}$$

$$\varepsilon_1 = \frac{2\log(1 + 2/\varepsilon)}{(1-\varepsilon)^2}, \; \varepsilon_2 = \frac{2}{(1-\varepsilon)^2}. \tag{7}$$

Remark 1: In general, the choice of ε_1,ε_2 based on (7) is not necessarily optimal. For instance, when the state dimension $n = 1$, one can choose $\varepsilon_1 = 2\log 2$ and $\varepsilon_2 = 2$ by Hoeffding's Inequality [23, Ch. 1] for a tighter bound.

Based on Proposition 1, we establish a probabilistic bound on the stochastic trajectory gap over a finite horizon.

Theorem 2 (Stochastic Trajectory Gap): Consider the stochastic system (1) and its associated deterministic system (2) under Assumptions 1 and 2. Let X_t be the trajectory of (1) and x_t be the associated trajectory of (2). For any given $\delta \in (0, 1]$ and desired $\varepsilon \in (0, 1)$, define

$$r_{\delta,t} = \sqrt{\Psi_t(\varepsilon_1 n + \varepsilon_2 \log(\tfrac{T}{\delta}))}, \tag{8}$$

where Ψ_t is as in (6) and $\varepsilon_1, \varepsilon_2$ are as in (7). Then

$$\mathbb{P}\big(\|X_t - x_t\| \leq r_{\delta,t}, \;\; \forall t \leq T\big) \geq 1 - \delta. \tag{9}$$

Proof: Given $0 \leq t \leq T$, Proposition 1 implies that for any associated X_t and x_t at time t, it holds that

$$\mathbb{P}\left(\|X_t - x_t\| > \sqrt{\Psi_t(\varepsilon_1 n + \varepsilon_2 \log(\tfrac{T}{\delta}))}\right) \leq \tfrac{\delta}{T}, \tag{10}$$

where Ψ_t is as in (6) and $\varepsilon_1, \varepsilon_2$ are as in (7). Define $r_{\delta,t} = \sqrt{\Psi_t(\varepsilon_1 n + \varepsilon_2 \log(\tfrac{T}{\delta})}$. Applying union bound inequality to (10) over $t = 1, \ldots, T$ yields

$$\mathbb{P}\left(\bigcap_{t=1}^{T} \|X_t - x_t\| \leq r_{\delta,t}\right) = 1 - \mathbb{P}\left(\bigcup_{t=1}^{T} \|X_t - x_t\| > r_{\delta,t}\right)$$
$$\geq 1 - \sum_{t=1}^{T} \frac{\delta}{T} = 1 - \delta,$$

which completes the proof. ■

For the special case when $L_t \equiv L$ and $\sigma_t \equiv \sigma$ with some $L, \sigma > 0$ for every $t \leq T$, the expression for $r_{\delta,t}$ in Theorem 2 can be simplified as follows:

$$r_{\delta,t} = \sqrt{\tfrac{\sigma^2(L^{2t}-1)}{L^2-1}\big(\varepsilon_1 n + \varepsilon_2 \log\big(\tfrac{T}{\delta}\big)\big)}. \tag{11}$$

Compared to the single-time probabilistic bound (5), $r_{\delta,t}$ derived in Theorem 2 is more conservative due to the application of union bound inequality among the whole trajectory. However, the union bound only leads to an additional $\mathcal{O}(\sqrt{\log T})$ term, which scales sufficiently slow with T (e.g., $\sqrt{\log T} = 4.80$ when $T = 10^{10}$). Moreover, the bound (5) is proved to have the tightest dependence on n and $\frac{1}{\delta}$ for the stochastic system (1), and is exact for linear systems [1, Sec. 4.4]. Therefore, $r_{\delta,t}$ in (8) is overall a sharp probabilistic bound on stochastic trajectory gap. A comparison with some existing methods is displayed in Section VI, showing that our result is much tighter.

B. Probabilistic Bound by Worst-Case Analysis

The worst-case analysis is a commonly-used method for safety verification when the disturbance is bounded [6], [24]. It can also be applied to stochastic systems to estimate stochastic trajectory gap under any sub-Gaussian stochastic disturbance w_t. This is achieved by viewing w_t as a bounded disturbance with high probability. However, the result is more conservative than that in Theorem 2.

By the norm concentration properties of sub-Gaussian random variables [23, Chapter 1.4] and the union bound inequality, the bound

$$b_t = \sqrt{\sigma_t^2\big(\varepsilon_1 n + \varepsilon_2 \log\big(\tfrac{T}{\delta}\big)\big)} \tag{12}$$

for all $t \le T$ ensures that $\mathbb{P}(\|w_t\| \le b_t,\ \forall t \le T) \ge 1 - \delta$. A worst-case probabilistic bound on $\|X_t - x_t\|$ can be established by assuming this bound (12). More specifically, by the local Lipschitz assumption and the triangular inequality,

$$\begin{aligned}\|X_{t+1} - x_{t+1}\| &\le \|f(X_t, d_t, t) - f(x_t, d_t, t)\| + \|w_t\| \\ &\le L_t\|X_t - x_t\| + b_t\end{aligned}$$

for all $t < T$ with probability at least $1 - \delta$. It follows that

$$\|X_t - x_t\| \le \sqrt{\psi_{t-1}} \sum_{k=0}^{t-1} b_k \sqrt{\psi_k^{-1}}, \tag{13}$$

where ψ_t is as in (6). Plugging (12) into (13), we conclude

$$\|X_t - x_t\| \le \sqrt{\psi_{t-1}} \sum_{k=0}^{t-1} \sigma_k \sqrt{\psi_k^{-1}\big(\varepsilon_1 n + \varepsilon_2 \log\big(\tfrac{T}{\delta}\big)\big)},\ \ \forall t \le T \tag{14}$$

holds with probability at least $1 - \delta$.

This bound (14) derived using the worst-case analysis is substantially more conservative than that in Theorem 2. Indeed, since $\sqrt{\Psi_t} \le \sqrt{\psi_{t-1}} \sum_{k=0}^{t-1} \sigma_k \sqrt{\psi_k^{-1}}$ by (6), (14) is always worse than (8)-(9). To see more clearly the gap, consider the case when $L_t \equiv L$ and $\sigma_t \equiv \sigma$. In this case, (14) reduces to $\|X_t - x_t\| \le \frac{L^t - 1}{L - 1}\sqrt{\sigma^2(\varepsilon_1 n + \varepsilon_2 \log\frac{T}{\delta})}$, which is much worse than (11), especially when $L \approx 1$ or ≥ 1. The gap between (8) (the bound derived in Theorem 2) and (13) (worst-case analysis bound) arises from two estimates: i) $\|w_t\| \le b$, and ii) the triangle inequality $\|X_{t+1} - x_{t+1}\| \le \|f(X_t, d_t, t) - f(x_t, d_t, t)\| + \|w_t\|$. In fact, for both of these estimates, the equality holds rarely considering the randomness of the disturbance.

V. Set Erosion With Barrier Functions

By combining the set-erosion strategy in Theorem 1 with the probabilistic bound on the stochastic trajectory gap developed in Theorem 2, the stochastic system (1) starting from $\mathcal{X}_0 \subseteq \mathcal{C}$ can be verified to be safe with $1 - \delta$ guarantee, if

$$\begin{aligned} x_0 \in \mathcal{X}_0 \Rightarrow x_t \in \mathcal{C} \ominus \mathcal{B}^n\big(r_{\delta,t}, 0\big),\ \ r_{\delta,t} \text{ is as (8)}, \\ \forall d_t \in \mathcal{D}\ \forall t \le T. \end{aligned} \tag{15}$$

The new formulation (15) converts the stochastic safety verification problem into a deterministic safety verification on a time-varying set. It offers tremendous flexibility to Problem 1 as one can leverage any deterministic safety verification methods to verify (15). In applications, a large number of existing approaches for safety verification of deterministic systems are based upon barrier functions [6], [25]. In this section, we examplify (15) with the exponential barrier function.

The notion of discrete-time exponential barrier function is proposed in the literature [25]. Given a time-varying set $\tilde{\mathcal{C}}_t \subseteq \mathbb{R}^n$, we generalize this notion and introduce the discrete-time time-varying exponential barrier function (TV-EBF) for the set $\tilde{\mathcal{C}}_t$.

Definition 3 (TV-EBF): Consider the deterministic system (2) with $d_t \in \mathcal{D}$, $\mathcal{D} \subseteq \mathbb{R}^m$. Given a terminal time T, if there exists a smooth function $h(x, t) : \mathbb{R}^n \times \mathbb{N}_+ \to \mathbb{R}$ such that for any $t \le T$:

1) $\tilde{\mathcal{C}}_t = \{x \in \mathbb{R}^n : h(x, t) \ge 0\}$, and
2) there exists $\gamma \in (0, 1]$ such that, for all $d \in \mathcal{D}$,

$$h(f(x, d, t), t + 1) \ge (1 - \gamma)h(x, t),\ \ \text{forall}x \in \tilde{\mathcal{C}}_t.$$

Then $h(x, t)$ is a *discrete-time time-varying exponential barrier function (TV-EBF)* for the set $\tilde{\mathcal{C}}_t$.

When $\mathcal{X}_0 \subseteq \mathcal{C}$ and $\tilde{\mathcal{C}}_t \subseteq \mathcal{C} \ominus \mathcal{B}^n(r_{\delta,t}, 0)$, the existence of $h(x, t)$ on $\tilde{\mathcal{C}}_t$ given as Definition 3 guarantees that the deterministic system (2) is safe. Therefore, the set-erosion strategy in (15) implies that the stochastic system (1) is safe with $1 - \delta$ guarantee. This result is formalized as follows.

Proposition 2 (Safety Using TV-EBF): Consider the stochastic system (1) with the initial configuration $\mathcal{X}_0 \subseteq \mathbb{R}^n$, the disturbance set $\mathcal{D} \subseteq \mathbb{R}^m$ and its associated deterministic system (2) under Assumptions 1 and 2. Given a safe set $\mathcal{C} \subseteq \mathbb{R}^n$ and terminal time T, define $r_{\delta,t}$ as (8). If $X_0 \in \mathcal{X}_0 \subseteq \mathcal{C}$ and there exists a $\tilde{\mathcal{C}}_t$ such that $\tilde{\mathcal{C}}_t \subseteq \mathcal{C} \ominus \mathcal{B}^n(r_{\delta,t}, 0)$ and a TV-EBF $h(x, t)$ as defined in Definition 3 on $\tilde{\mathcal{C}}_t$ for the deterministic system (2), then the stochastic system (1) is safe with $1 - \delta$ guarantee on $\mathcal{C}$.

Proof: Clearly it holds that $h(x_t, t) \ge (1 - \gamma)^t h(x_0, 0)$ for any $t \le T$. Since $x_0 \in \mathcal{X}_0 \subseteq \tilde{\mathcal{C}}_0$, this implies that $h(x_t, t) \ge 0$, for every $t \le T$, and therefore $x_t \in \tilde{\mathcal{C}}_t$, for every $t \le T$. Since $\tilde{\mathcal{C}}_t \subseteq \mathcal{C} \ominus \mathcal{B}^n(r_{\delta,t}, 0)$, x_t satisfies the set-erosion strategy in (15), which suffices to show that the stochastic system (1) is safe with $1 - \delta$ guarantee on $\mathcal{C}$. ■

Since $r_{\delta,t}$ as (8) is sharp, Proposition 2 provides an effective stochastic safety verification scheme based on deterministic barrier certifications. Its efficiency depends on the calculation of the Minkowski difference $\mathcal{C} \ominus \mathcal{B}^n(r_{\delta,t}, 0)$. Notice that $\mathcal{C} \ominus \mathcal{B}^n(r_{\delta,t}, 0) = (\mathcal{C}^c \oplus \mathcal{B}^n(r_{\delta,t}, 0))^c$, where the complement $\mathcal{C}^c$ of $\mathcal{C}$ is treated as the unsafe set. Thus, Proposition 2 can be considered a barrier certification for the obstacle avoidance task with "time-dependent expanded obstacles" $\mathcal{C}^c \oplus \mathcal{B}^n(r_{\delta,t}, 0)$, which has been well-studied [26], [27]. When $\mathcal{C}^c$ is the union of convex sets such as ellipsoids or polygons, $\mathcal{C}^c \oplus \mathcal{B}^n(r_{\delta,t}, 0)$ can be efficiently computed [28].

VI. Case Studies

In this section, we present two examples to validate the proposed safety verification method. In the first example, we verify safety of a linear scalar stochastic system on a finite interval. In the second example, we verify safety of unicycle model of a vehicle with a stabilizing feedback controller.

A. Safety of Linear Systems Over an Interval

As the first experiment, we consider the following linear stochastic system

$$X_{t+1} = 0.99X_t + w_t,\ \ X_0 = 0, \tag{16}$$

where $X_t \in \mathbb{R}$ and $w_t \sim \mathcal{N}(0, 10^{-3})$. This linear system satisfies Assumption 1 with $L_t \equiv L = 0.99$ and Assumption 2 with $\sigma_t^2 \equiv \sigma^2 = 10^{-3}$. The probabilistic bound $r_{\delta,t}$ on

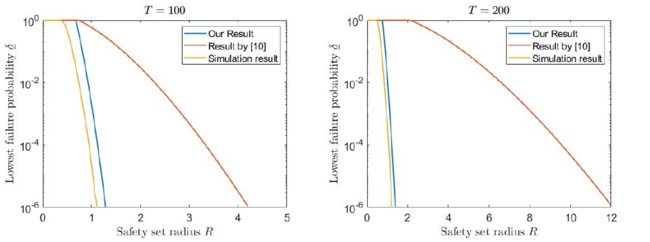

Fig. 2. The probability $\underline{\delta}$ (the lower the safer) that a strategy cannot guarantee safety of (16) on the centered ball with radius R during $t \le T$. The blue curve is given by our strategy (17), the yellow curve is the simulated result from 3×10^6 sampled trajectories, and the red curve is the baseline we choose, given by the main result of [10, Corollary 1]. **Left:** $T = 100$. **Right:** $T = 200$.

stochastic trajectory gap can be calculated by (11) with $\varepsilon_1 = 2\log 2$ and $\varepsilon_2 = 2$ by Remark 1.

The task is to verify the safety of the linear system (16) with $1-\delta$ guarantee on the interval $\mathcal{C} = \{x \in \mathbb{R} : |x| \le R\}$ during $t \le T$. Notice that by fixing $X_0 = 0$, the associated deterministic trajectory of the system (16) is $x_t \equiv 0$, and $\mathcal{B}^1(R,0) \ominus \mathcal{B}^1(r_{\delta,t},0) = \mathcal{B}^1(R - r_{\delta,t},0)$. Therefore, by our set-erosion strategy in (15), it is enough to verify whether $R \ge r_{\delta,t}$ for any $t \le T$. Since $r_{\delta,t}$ calculated by (11) is increasing with t, we conclude that it suffices to verify if $R \ge r_{\delta,T}$, which is equivalent to:

$$\delta \ge T \cdot \exp\left\{-\left(\frac{R^2\left(L^2-1\right)}{2\sigma^2\left(L^{2T}-1\right)} - \log 2\right)\right\}. \tag{17}$$

The right-hand side of (17) is the lowest probability $\underline{\delta}$ that our strategy (15) cannot guarantee safety for the linear system (16). When $\underline{\delta} \ge 1$, it means that the radius R of $\mathcal{C}$ is so small that the system (16) is considered unsafe on $\mathcal{C}$. In such a scenario we set $\delta = 1$. Figure 2 shows the relationship between $\underline{\delta}$ and R determined by (17). Our result is compared with the curve derived from [10, Corollary 1], which calculates $\underline{\delta}$ by upper bounding $\mathbb{P}(\min_{t\le T} x_t < -R)$, and is the best existing result for general dynamical systems to the best of our knowledge. We also compare with the simulated result given by Monte-Carlo approximations with 3×10^6 sampled trajectories. When R is very small, our strategy directly implies that the system is unsafe on $\mathcal{C}$, as suggested by the simulated result. When R gets larger, our strategy offers a result close to the simulated result and significantly sharper than existing methods. To show the tightness of the failure guarantees obtained from using method, we choose $R = 1.0$ for $T = 100$ and $R = 1.08$ for $T = 200$, both of which should guarantee $\underline{\delta} = 10^{-3}$ if our result shown in Figure 2 is correct. Then we sample 5000 independent stochastic trajectories of (16) in both cases, and visualize their absolute values in Figure 3. All the trajectories of $|X_t|$ are within the bound R and some trajectories get quite close to the boundary of the safe set, validating our result.

B. Nonlinear Unicycle System

Next, we consider a unicycle moving on a 2-dimensional plane with obstacles. The unsafe region $\mathcal{C}_u = \{(p_x - 1.3)^2 + (p_y - 3.5)^2 \le 0.9^2\} \cup \{(p_x + 0.3)^2 + (p_y - 2)^2 \le 0.72^2\} \cup \{(p_x - 6.2)^2 + (p_y - 0.5)^2 \le 0.75^2\}$ is the union of red obstacles shown in Figure 4 and the safe region is $\mathcal{C} = \mathbb{R}^n \setminus \mathcal{C}_u$. The discrete-time system model is given as

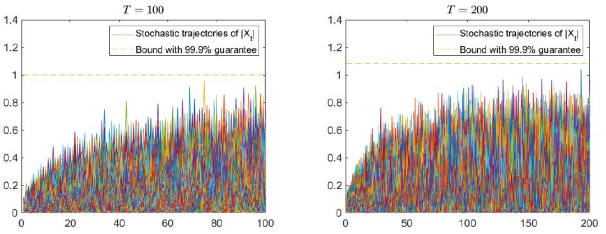

Fig. 3. 5000 sampled stochastic trajectories of (16) with R that corresponds to $\underline{\delta} = 10^{-3}$ in blue curves (our result) of Figure 2. **Left:** $T = 100$. **Right:** $T = 200$.

$$\begin{aligned} X_{t+1} &= X_t + \eta \begin{bmatrix} v_t(X_t)\cos(\theta_t) \\ v_t(X_t)\sin(\theta_t) \\ \omega_t(X_t) + d_t \end{bmatrix} + w_t \\ &= f(X_t, d_t) + w_t, \end{aligned} \tag{18}$$

where $X_t = \begin{bmatrix} p_{x,t} & p_{y,t} & \theta_t \end{bmatrix}^\mathsf{T}$ is the state of the vehicle, $(p_{x,t}, p_{y,t})$ is the position of the center of mass of the vehicle in the plane, θ_t is the heading angle of the vehicle, $v_t(X_t)$ is the velocity of the center of mass, $\omega_t(X_t)$ is the angular velocity of the vehicle, η is the discretization step size, d_t is a bounded disturbance on the angular velocity, and w_t is the stochastic disturbance on the model. In this experiment, we assume that $|d_t| \le 0.1$, $w_t \sim \sqrt{\eta} \cdot \mathcal{N}(0, 0.02 I_3)$, $\eta = 0.01$. $v_t(X_t)$ and $\omega_t(X_t)$ are designed as the feedback controllers proposed in [29]. The task of the unicycle is to reach the origin point while avoiding the obstacles under both d_t and w_t. The details of controller design can be found in [22, Sec. VIII].

Our goal is to verify the safety of the stochastic system (18) with $1-\delta$ guarantee through the set erosion strategy. We set $\delta = 10^{-4}$ and the initial state set $\mathcal{X}_0 = \begin{bmatrix} 5 & 5 & -\frac{\pi}{3} \end{bmatrix}^\mathsf{T} \pm 0.1$. The probabilistic bound $r_{\delta,t}$ is calculated as (8) with $\varepsilon = 1/16$, and L_t estimated by the methods proposed in [30]. Define $r_m = \max_{t\le T} r_{\delta,t}$, then by the set erosion strategy (15), it suffices to verify whether for the associated deterministic system of (18), $x_t \in \mathcal{C} \ominus \mathcal{B}^n(r_m, 0)$ holds for any x_t starting from $x_0 \in \mathcal{X}_0$ and under any $|d_t| \le 0.1$. We use barrier certification to verify this condition, where Proposition 2 reduces to time-independent barrier certification for forward-invariant condition [8]. The tool we use is FOSSIL developed by [31]. Based on the experiment setting, this program returns "`Found a valid BARRIER certificate`", implying that the safety of the system (18) with $1-\delta$ guarantee on the zero-superlevel set of this barrier function is verified.

To visualize the set-erosion strategy, we simulate 5000 independent trajectories of the associated deterministic system from $x_0 \in \mathcal{X}_0$ with $T = 100, 500$ separately. The results are shown in the left column of Figure 4. The areas in yellow are the eroded parts $\mathcal{C} \setminus (\mathcal{C} \ominus \mathcal{B}^n(r_m, 0))$ of the $\mathcal{C}$. It is clear that all the deterministic trajectories have no intersections with the yellow areas. Meanwhile, to validate the effectiveness of our strategy, we sample 20000 independent trajectories of the stochastic system (18) from $X_0 \in \mathcal{X}_0$ during $t \le T$. It is clear that all the stochastic trajectories successfully avoid all the obstacles, satisfying our safety verification strategy.

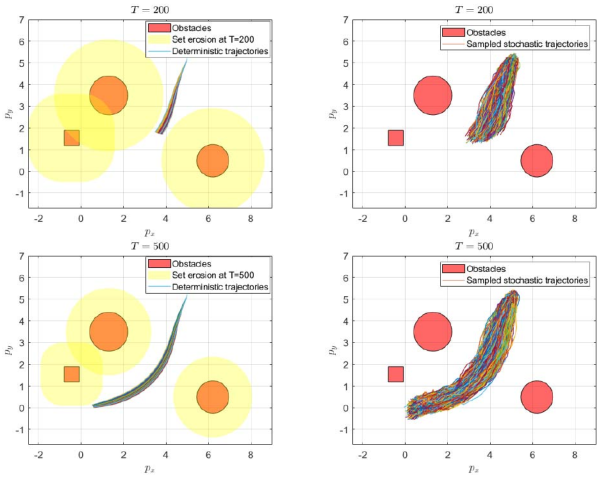

Fig. 4. Stochastic safety verification of the unicycle system (18) with **99.99%** guarantee. **Left:** Stochastic safety verification using the set-erosion strategy at the terminal time $T = 100, 500$. The red shapes are obstacles. The yellow areas are the eroded part $\mathcal{C}\backslash(\mathcal{C} \ominus \mathcal{B}^n(r_m, 0))$. Each curve is an independent trajectory of the associated deterministic unicycle system with different d_t. **Right:** Simulation of the stochastic trajectories. Each curve is an independently sampled trajectory of the stochastic system (18) during $t \leq T$, $T = 100, 500$.

VII. Conclusion

We propose a general approach called set-erosion strategy for safety verification of discrete-time stochastic systems with sub-Gaussian disturbances. Our set-erosion strategy reduces the problem of safety verification of discrete-time stochastic systems into the safety verification of an associated deterministic system on an eroded subset of the safe set. Based on our results in [1], we provide a sharp probabilistic bound on the depth of this erosion. This approach brings tremendous flexibility to the safety verification of stochastic systems as any deterministic safety verification methods can be used to ensure safety on the eroded subset of the safe set. In particular, we consider the exponential barrier function for safety verification of deterministic systems and leverage it to obtain efficient stochastic safety verification schemes.

References

[1] Z. Liu, S. Jafarpour, and Y. Chen, "Probabilistic reachability of discrete-time nonlinear stochastic systems," 2024, *arXiv:2409.09334*.

[2] B. Li, S. Wen, Z. Yan, G. Wen, and T. Huang, "A survey on the control lyapunov function and control barrier function for nonlinear-affine control systems," *IEEE/CAA J. Automatica Sinica*, vol. 10, no. 3, pp. 584–602, Mar. 2023.

[3] M. Zhang, B. Selic, S. Ali, T. Yue, O. Okariz, and R. Norgren, "Understanding uncertainty in cyber-physical systems: A conceptual model," in *Proc. Eur. Conf. Model. Found. Appl.*, 2016, pp. 247–264.

[4] A. Abate, M. Prandini, J. Lygeros, and S. Sastry, "Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems," *Automatica*, vol. 44, no. 11, pp. 2724–2734, 2008.

[5] S. Summers and J. Lygeros, "Verification of discrete time stochastic hybrid systems: A stochastic reach-avoid decision problem," *Automatica*, vol. 46, no. 12, pp. 1951–1961, 2010.

[6] S. Prajna, A. Jadbabaie, and G. J. Pappas, "A framework for worst-case and stochastic safety verification using barrier certificates," *IEEE Trans. Autom. Control*, vol. 52, no. 8, pp. 1415–1428, Aug. 2007.

[7] S. Kolathaya and A. D. Ames, "Input-to-state safety with control barrier functions," *IEEE Control Syst. Lett.*, vol. 3, pp. 108–113, 2019.

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

[9] M. P. Chapman, R. Bonalli, K. M. Smith, I. Yang, M. Pavone, and C. J. Tomlin, "Risk-sensitive safety analysis using conditional value-at-risk," *IEEE Trans. Autom. Control*, vol. 67, no. 12, pp. 6521–6536, Dec. 2022.

[10] R. K. Cosner, P. Culbertson, and A. D. Ames, "Bounding stochastic safety: Leveraging freedman's inequality with discrete-time control barrier functions," 2024, *arXiv:2403.05745*.

[11] Y. Nishimura and K. Hoshino, "Control barrier functions for stochastic systems and safety-critical control designs," *IEEE Trans. Autom. Control*, vol. 69, no. 11, pp. 8088–8095, Nov. 2024.

[12] C. Santoyo, M. Dutreix, and S. Coogan, "A barrier function approach to finite-time stochastic system verification and control," *Automatica*, vol. 125, Mar. 2021, Art. no. 109439.

[13] J. Steinhardt and R. Tedrake, "Finite-time regional verification of stochastic non-linear systems," *Int. J. Robot. Res.*, vol. 31, no. 7, pp. 901–923, 2012.

[14] K. M. Frey, T. J. Steiner, and J. P. How, "Collision probabilities for continuous-time systems without sampling [with appendices]," 2020, *arXiv:2006.01109*.

[15] L. Blackmore and M. Ono, "Convex chance constrained predictive control without sampling," in *Proc. AIAA Guid., Navig., control Conf.*, 2009, p. 5876.

[16] M. Ono, M. Pavone, Y. Kuwata, and J. Balaram, "Chance-constrained dynamic programming with application to risk-aware robotic space exploration," *Auton. Robots*, vol. 39, pp. 555–571, Dec. 2015.

[17] E. E. Vlahakis, L. Lindemann, P. Sopasakis, and D. V. Dimarogonas, "Probabilistic tube-based control synthesis of stochastic multi-agent systems under signal temporal logic," 2024, *arXiv:2405.02827*.

[18] L. Blackmore, M. Ono, and B. C. Williams, "Chance-constrained optimal path planning with obstacles," *IEEE Trans. Robot.*, vol. 27, no. 6, pp. 1080–1094, Dec. 2011.

[19] B. Gopalakrishnan, A. K. Singh, M. Kaushik, K. M. Krishna, and D. Manocha, "PRVO: Probabilistic reciprocal velocity obstacle for multi robot navigation under uncertainty," in *Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst. (IROS)*, 2017, pp. 1089–1096.

[20] J. Köhler and M. N. Zeilinger, "Predictive control for nonlinear stochastic systems: Closed-loop guarantees with unbounded noise," 2024, *arXiv:2407.13257*.

[21] R. Vershynin, *High-Dimensional Probability: An Introduction with Applications in Data Science* (Cambridge Series in Statistical and Probabilistic Mathematics). Cambridge, U.K.: Cambridge Univ., 2018.

[22] S. Jafarpour, Z. Liu, and Y. Chen, "Probabilistic reachability analysis of stochastic control systems," 2024, *arXiv:2407.12225*.

[23] P. Rigollet and J.-C. Hütter, "High-dimensional statistics," 2023, *arXiv:2310.19244*.

[24] C. Novara, L. Fagiano, and M. Milanese, "Direct feedback control design for nonlinear systems," *Automatica*, vol. 49, no. 4, pp. 849–860, 2013.

[25] A. Agrawal and K. Sreenath, "Discrete control barrier functions for safety-critical control of discrete systems with application to bipedal robot navigation," in *Proc. Robot., Sci. Syst.*, vol. 13, 2017, pp. 1–10.

[26] I. Tezuka and H. Nakamura, "Time-varying obstacle avoidance by using high-gain observer and input-to-state constraint safe control barrier function," *IFAC-PapersOnLine*, vol. 53, no. 5, pp. 391–396, 2020.

[27] T. G. Molnar, A. K. Kiss, A. D. Ames, and G. Orosz, "Safety-critical control with input delay in dynamic environment," *IEEE Trans. Control Syst. Technol.*, vol. 31, no. 4, pp. 1507–1520, Jul. 2023.

[28] C. Weibel, *Minkowski Sums of Polytopes: Combinatorics and Computation*, EPFL, Lausanne, Switzerland, 2007.

[29] M. Aicardi, G. Casalino, A. Bicchi, and A. Balestrino, "Closed loop steering of unicycle like vehicles via Lyapunov techniques," *IEEE Robot. Autom. Mag.*, vol. 2, no. 1, pp. 27–35, Mar. 1995.

[30] C. Fan, J. Kapinski, X. Jin, and S. Mitra, "Simulation-driven reachability using matrix measures," *ACM Trans. Embed. Comput. Syst.*, vol. 17, no. 1, pp. 1–28, Dec. 2017. [Online]. Available: https://doi.org/10.1145/3126685

[31] A. Abate, D. Ahmed, A. Edwards, M. Giacobbe, and A. Peruffo, "FOSSIL: A software tool for the formal synthesis of Lyapunov functions and barrier certificates using neural networks," in *Proc. 24th Int. Conf. Hybrid Syst., Comput. Control*, 2021, pp. 1–11.