2024 IEEE 63rd Conference on Decision and Control (CDC)
December 16-19, 2024. MiCo, Milan, Italy

Safe Exit Controllers Synthesis for Continuous-time Stochastic Systems

Bai Xue, *IEEE Member*

***Abstract*— This paper tackles the problem of generating safe exit controllers for continuous-time systems described by stochastic differential equations (SDEs). The primary aim is to develop controllers that maximize the lower bounds of the exit probability that the system escapes from a safe but uncomfortable set within a specified time frame and guide it towards a comfortable set. The paper considers two distinct cases: one in which the boundary of the safe set is a subset of the boundary of the uncomfortable set, and the other where the boundaries of the two sets do not intersect. To begin, we present a sufficient condition for establishing lower bounds on the exit probability in the first case. This condition serves as a guideline for constructing a point-wise optimization using linear programs. The linear programming problem is designed to implicitly synthesize an optimal exit controller online that maximizes the lower bounds of the exit probability. The method employed in the first case is then extended to the second one. Finally, we demonstrate the effectiveness of the proposed approaches on one example.**

I. Introduction

Stochastic systems are highly significant in various fields such as robotics, finance, and biology due to their ability to model uncertain factors that can greatly influence system behavior. Stochastic differential equations (SDEs) provide a powerful modeling approach for such systems as they allow for the incorporation of inherent uncertainties in system dynamics [1]. This enables the analysis of system behavior, as well as the verification of properties related to safety, reliability, and performance.

In recent years, there has witnessed an increased focus on safety properties [2], [3], [4], particularly in the context of safety-critical systems. Safety verification via barrier certificates for stochastic systems with infinite time horizons was introduced in [5] alongside the deterministic counterpart. This framework builds upon the known Doob's nonnegative supermartingale inequality (or, Ville's inequality [6]) and enables bounding the exit probability from above, indicating the likelihood of a system leaving a safe region. However, this approach has a limitation as it requires the infinitesimal generator, responsible for the expected value evolution of a stochastic process, to be nonpositive. Consequently, the barrier function is restricted to be a supermartingale. To overcome this restriction, [7] relaxed the condition by introducing barrier certificates based on c-martingales. A c-martingale allows the expected value of the barrier function to increase over time while providing an upper bound on the infinitesimal generator. This approach provides upper bounds of the exit probability for systems with finite time horizons. Afterwards, inspired by studies in [8], [9] enhanced the c-martingales and proposed a barrier certificate constraint that imposes a state-dependent bound on the infinitesimal generator for upper-bounding the exit probability with finite time horizons. Moreover, a sum-of-squares optimization based method was proposed in [9] to synthesizing polynomial state feedback controllers. Further contributions to the computation of upper bounds of the exit probability include [10], which presented a comparison theorem for one-dimensional SDEs and applied it to upper-bound exit probabilities for multi-dimensional SDEs in terms of an exit probability of a one-dimensional process. Recently, based on online convex quadratic programs that synthesize controllers implicitly [11], [12], [13] introduced stochastic control barrier functions as a framework for synthesizing controllers that enforce upper bounds on exit probabilities over both infinite and finite time horizons. The conditions for upper-bounding exit probabilities in the aforementioned works, except [10], are constructed or derived from the Doob's nonnegative supermartingale inequality.

On the other hand, in [14], a novel approach was proposed for characterizing the exact reachability probability of discrete-time stochastic systems. This probability measures the likelihood of a system starting from an initial set and eventually entering target sets, while staying within safe sets before the first target hitting time. Unlike previous methods that rely on Doob's nonnegative supermartingale inequality, this approach derives an equation that provides an exact estimation of the reachability probability [15]. By relaxing this equation, barrier-like conditions can be obtained to both lower-bound and upper-bound the reachability probability. Additionally, the method has been extended in [16] to compute lower and upper bounds of the exit probability over an infinite time horizon for discrete-time stochastic systems. Furthermore, the equation and its relaxations have been further extended in [17] to perform reach-avoid analysis over infinite-time horizons for systems modeled by SDEs. The use of sum-of-squares optimization techniques has enabled the application of these barrier-like conditions in the synthesis of controllers for safety-critical systems, as in [18].

In safety-focused applications, it is common to prioritize the computation of upper bounds for the exit probability from a safe set. However, there is a significant lack of methods specifically focused on computing lower bounds, despite their significance in certain practical scenarios. Consider a situation where a system operates within a safe set but

This work is funded by the CAS Pioneer Hundred Talents Program and Basic Research Program of Institute of Software, CAS (Grant No. ISCAS-JCMS-202302).

Key Laboratory of System Software (Chinese Academy of Sciences) and State Key Lab. of Computer Science, Institute of Software, CAS, Beijing, China {xuebai@ios.ac.cn}

University of Chinese Academy of Sciences, Beijing, China

experiences discomfort, such as a robotic system navigating around the boundary of the safe set. Although the system is safe, it may encounter discomfort due to the fragility of safety violations. In this situation, the system would prefer to leave this typical safe set to alleviate the discomfort. By maximizing lower bounds of the exit probability, we can ensure that the system has a higher probability of safely leaving this uncomfortable set and reaching a safe set that provides more comfort. It not only ensures safety but also considers comfort, resulting in a more holistic solution for safety-focused applications. This aspect becomes increasingly important for systems like autonomous vehicles, where comfort plays a substantial role once safety requirements are met. Additionally, considering lower bounds can complement existing methods that focus on computing upper bounds of the exit probability, and thus can provide us a more comprehensive analysis of the system's behavior.

In this paper, we investigate the problem of generating safe controllers that optimize the lower bounds of exit probabilities for continuous-time systems represented by SDEs over both bounded and unbounded time horizons. The exit probability refers to the likelihood of a system, starting from an open, safe but uncomfortable set (which is a subset of the safe set), exiting that set within a specified bounded/unbounded time frame and entering a comfortable set. We analyze two different cases in this study. In the first case, the boundary of the safe set is a subset of the boundary of the uncomfortable set. We begin by establishing a sufficient condition for lower-bounding the exit probability in this case, extending the condition presented in [18]. Based on the proposed sufficient condition, we formulate an online linear programming problem to synthesize an optimal controller implicitly that maximizes lower bounds of the exit probability. Then we extend the sufficient condition and linear programming method in the first case to the second one, in which the boundary of the safe set does not intersect with the boundary of the uncomfortable set. Finally, to illustrate the effectiveness of our proposed methods, we provide an example and demonstrate their applicability.

The main contribution of our work is summarized as follows: unlike previous studies that primarily focused on synthesizing controllers to enforce upper bounds on the exit probability for systems modeled by SDEs, the present work introduces novel conditions for controller synthesis that specifically provide lower bounds of the exit probability. These conditions are applicable to both finite and infinite time horizons in exit analysis. One key aspect of our contribution is that our proposed conditions not only extend the existing condition presented in [18] to the finite-time scenario but also encompass it as a special case within our framework. This demonstrates the versatility of our conditions in handling a wider range of scenarios compared to the one in [18].

This paper is structured as follows. In Section II, we introduce SDEs and the problems of synthesizing safe exit controllers. In Section III, we present our sufficient conditions for characterizing lower bounds of the exit probabilities and our linear programming methods for synthesizing controllers that maximize these lower bounds. In Section IV, we demonstrate the effectiveness of our approach through one example. Finally, in Section V, we conclude the paper and discuss avenues for future research.

Some basic notions are used in this paper: $\mathbb{R}$ and $\mathbb{R}_{\geq 0}$ stand for the set of real numbers and non-negative real numbers, respectively; $\mathbb{R}^n$ and $\mathbb{R}^{n\times m}$ denote the space of all n-dimensional vectors and $n \times m$ real matrices, respectively; for a set $\mathcal{A}$, $\overline{\mathcal{A}}$ and $\partial\mathcal{A}$ denotes the closure and boundary of the set $\mathcal{A}$, respectively; $\wedge$ denotes the logical operation of conjunction.

II. Preliminaries

This section introduces SDEs and the exit controllers synthesis problem of interest.

Consider an affine stochastic control system,

$$d\boldsymbol{x}(t,\boldsymbol{w}) = (\boldsymbol{f}_1(\boldsymbol{x}(t,\boldsymbol{w}))+\boldsymbol{f}_2(\boldsymbol{x}(t,\boldsymbol{w}))\boldsymbol{u}(\boldsymbol{x}(t)))dt + \boldsymbol{\sigma}(\boldsymbol{x}(t,\boldsymbol{w}))d\boldsymbol{W}(t,\boldsymbol{w}), \tag{1}$$

where $\boldsymbol{f}_1(\cdot) : \mathbb{R}^n \to \mathbb{R}^n$, $\boldsymbol{f}_2(\cdot) : \mathbb{R}^n \to \mathbb{R}^{n\times m}$, and $\boldsymbol{\sigma}(\cdot) : \mathbb{R}^n \to \mathbb{R}^{n\times k}$ are locally Lipschitz continuous function; the admissible input is defined by the function $\boldsymbol{u}(\cdot) : \mathbb{R}^n \to \mathcal{U}$ with $\mathcal{U}$ being the admissible input set; $\boldsymbol{W}(t,\boldsymbol{w}) : \mathbb{R} \times \Omega \to \mathbb{R}^k$ is an k-dimensional Wiener process (standard Brownian motion), and Ω, equipped with the probability measure $\mathbb{P}$, is the sample space $\boldsymbol{w}$ belongs to. The expectation with respect to $\mathbb{P}$ is denoted by $\mathbb{E}[\cdot]$.

Given a locally Lipschitz controller $\boldsymbol{u}(\boldsymbol{x})$, for an initial state $\boldsymbol{x}_0$, the SDE (1) has a unique (maximal local) strong solution over a time interval $[0, T^{\boldsymbol{x}_0}(\boldsymbol{w}))$, where $T^{\boldsymbol{x}_0}(\boldsymbol{w})$ is a positive real value or infinity. This solution is denoted as $\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(\cdot) : [0, 0) \to \mathbb{R}^n$, which satisfies the stochastic integral equation,

$$\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t) = \int_0^t (\boldsymbol{f}_1(\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(\tau)) + \boldsymbol{f}_2(\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(\tau))\boldsymbol{u}(\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(\tau)))d\tau + \int_0^t \boldsymbol{\sigma}(\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(\tau))d\boldsymbol{W}(\tau,\boldsymbol{w}) + \boldsymbol{x}_0.$$

Also, given a function $v(\boldsymbol{x})$ that is twice continuously differentiable over $\boldsymbol{x}$, the infinitesimal generator underlying system (1) with this controller $\boldsymbol{u}(\boldsymbol{x})$, which represents the limit of the expected value of $v(\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t))$ as t approaches 0, is

$$\mathcal{L}_{v,\boldsymbol{u}}(\boldsymbol{x}_0) = \lim_{t\to 0} \frac{\mathbb{E}[v(\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t))] - v(\boldsymbol{x}_0)}{t} =$$
$$[\frac{\partial v}{\partial \boldsymbol{x}}(\boldsymbol{f}_1(\boldsymbol{x}) + \boldsymbol{f}_2(\boldsymbol{x})\boldsymbol{u}(\boldsymbol{x})) + \frac{1}{2}\mathbf{tr}(\boldsymbol{\sigma}(\boldsymbol{x})^\top \frac{\partial^2 v}{\partial \boldsymbol{x}^2}\boldsymbol{\sigma}(\boldsymbol{x}))] \mid_{\boldsymbol{x}=\boldsymbol{x}_0},$$

where $\frac{\partial v}{\partial \boldsymbol{x}}$ represents the gradient of the function $v(\boldsymbol{x})$ with respect to $\boldsymbol{x}$, and $\mathbf{tr}(\cdot)$ denotes the trace of a matrix.

Given a safe set $\mathcal{S} \subseteq \mathbb{R}^n$ and an uncomfortable set $\mathcal{C} \subseteq \mathcal{S}$, a safe exit controller is a controller that maximizes the exit probability of system (1), starting from $\mathcal{C}$, entering the comfortable set $\mathcal{S} \setminus \mathcal{C}$ within a specified time horizon. Additionally, it is required that the system remains inside $\mathcal{C}$ before leaving it.

Definition 1 (Safe Exit Controllers): Given a time horizon $\mathbb{T}$, an initial state $\boldsymbol{x}_0 \in \mathcal{C}$ and a probability threshold $p_{\boldsymbol{x}_0} \in [0,1]$, an exit controller is a locally Lipschitz controller $\boldsymbol{u}(\cdot) : \overline{\mathcal{C}} \to \mathbb{R}^m$ satisfying the following condition:

$$\mathbb{P}\left(\left\{\boldsymbol{w} \in \Omega \mid \begin{matrix} \exists t \in \mathbb{T}. \boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t) \in \mathcal{S} \setminus \mathcal{C} \bigwedge \\ \forall \tau \in [0,t). \boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(\tau) \in \mathcal{C} \end{matrix} \right\}\right) \geq p_{\boldsymbol{x}_0}, \quad (2)$$

where $\mathbb{T} = [0,T]$ if $T < \infty$, and $\mathbb{T} = [0,\infty)$ otherwise.

In Definition 1, the exit controller is related to a lower bound of the exact exit probability. The safe exit controllers synthesis problem of interest in this work is to synthesize an exit controller maximizing the threshold $p_{\boldsymbol{x}_0}$. The synthesis problem in this paper is considered in the following two distinct cases.

The first case we consider is that the boundary of the safe set $\mathcal{S}$ is a subset of the one of the uncomfortable set $\mathcal{C}$, i.e., $\partial\mathcal{S} \subseteq \partial\mathcal{C}$. Specifically, we assume $\mathcal{S} = \{\boldsymbol{x} \in \mathbb{R}^n \mid h(\boldsymbol{x}) > 0\}$ with $\partial\mathcal{S} = \{\boldsymbol{x} \in \mathbb{R}^n \mid h(\boldsymbol{x}) = 0\}$ and $\mathcal{C} = \{\boldsymbol{x} \in \mathbb{R}^n \mid 0 < h(\boldsymbol{x}) < 1\}$ with $\partial\mathcal{C} = \{\boldsymbol{x} \in \mathbb{R}^n \mid h(\boldsymbol{x}) = 0 \vee h(\boldsymbol{x}) = 1\}$. This assumption is made based on the practical consideration that a system operating close to the boundary of a safe set is at a higher risk of safety hazards, thereby making the system operation in this set uncomfortable. In this case, system (1) should be enforced to exit the set $\mathcal{C}$ through states satisfying $h(\boldsymbol{x}) = 1$ rather than $h(\boldsymbol{x}) = 0$. Thus, that $\exists t \in \mathbb{T}. \boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t) \in \mathcal{S} \setminus \mathcal{C} \wedge \forall \tau \in [0,t). \boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(\tau) \in \mathcal{C}$ is equivalent to $\exists t \in \mathbb{T}. h(\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t)) = 1 \wedge \forall \tau \in [0,t). \boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(\tau) \in \mathcal{C}$. The corresponding exit controllers synthesis problem is formulated in Definition 2.

Definition 2 (Safe Exit Controllers Synthesis Problem I): Assume the safe set is $\mathcal{S} = \{\boldsymbol{x} \in \mathbb{R}^n \mid h(\boldsymbol{x}) > 0\}$ with $\partial\mathcal{S} = \{\boldsymbol{x} \in \mathbb{R}^n \mid h(\boldsymbol{x}) = 0\}$ and the uncomfortable set $\mathcal{C} = \{\boldsymbol{x} \in \mathbb{R}^n \mid 0 < h(\boldsymbol{x}) < 1\}$ with $\partial\mathcal{C} = \{\boldsymbol{x} \in \mathbb{R}^n \mid h(\boldsymbol{x}) = 0 \vee h(\boldsymbol{x}) = 1\}$, where $h(\cdot) : \mathbb{R}^n \to \mathbb{R}$ is a twice continuously differentiable function. Given a time horizon $\mathbb{T}$, the safe exit controllers synthesis problem is to synthesize a locally Lipschitz controller $\boldsymbol{u}(\cdot) : \overline{\mathcal{C}} \to \mathbb{R}^m$ of maximizing lower bounds of the exit probability for system (1) leaving the set $\mathcal{C}$ through states in $\{\boldsymbol{x} \in \mathbb{R}^n \mid h(\boldsymbol{x}) = 1\}$, i.e., solving the following optimization problem:

$$\begin{aligned} &\max_{\boldsymbol{u}} p_{\boldsymbol{x}_0} \\ &\text{s.t. } \mathbb{P}\left(\left\{\boldsymbol{w} \in \Omega \mid \begin{matrix} \exists t \in \mathbb{T}. h(\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t)) = 1 \bigwedge \\ \forall \tau \in [0,t). \boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(\tau) \in \mathcal{C} \end{matrix} \right\}\right) \geq p_{\boldsymbol{x}_0}, \end{aligned} \quad (3)$$

where $\mathbb{T} = [0,T]$ if $T < \infty$, and $\mathbb{T} = [0,\infty)$ otherwise.

The second case we consider is that the boundary of the uncomfortable set $\mathcal{C}$ does not intersect the boundary of the safe set $\mathcal{S}$, i.e., $\partial\mathcal{S} \cap \partial\mathcal{C} = \emptyset$. In this case, we assume $\mathcal{S} = \{\boldsymbol{x} \in \mathbb{R}^n \mid h(\boldsymbol{x}) > 0\}$ with $\partial\mathcal{S} = \{\boldsymbol{x} \in \mathbb{R}^n \mid h(\boldsymbol{x}) = 0\}$ and $\mathcal{C} = \{\boldsymbol{x} \in \mathbb{R}^n \mid g(\boldsymbol{x}) < 1\}$ with $\partial\mathcal{C} = \{\boldsymbol{x} \in \mathbb{R}^n \mid g(\boldsymbol{x}) = 1\}$. In this case, that $\exists t \in [0,T]. \boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t) \in \mathcal{S} \setminus \mathcal{C} \wedge \forall \tau \in [0,t). \boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(\tau) \in \mathcal{C}$ is equivalent to $\exists t \in [0,T]. \boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t) \in \partial\mathcal{C} \wedge \forall \tau \in [0,t). \boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(\tau) \in \mathcal{C}$. Thus, the corresponding safe exit controllers synthesis problem is formulated in Definition 3.

Definition 3 (Safe Exit Controllers Synthesis Problem II): Assume the uncomfortable set is $\mathcal{C} = \{\boldsymbol{x} \in \mathbb{R}^n \mid g(\boldsymbol{x}) < 1\}$ with $\partial\mathcal{C} = \{\boldsymbol{x} \in \mathbb{R}^n \mid g(\boldsymbol{x}) = 1\}$ and $\partial\mathcal{S} \cap \partial\mathcal{C} = \emptyset$, where $g(\cdot) : \mathbb{R}^n \to \mathbb{R}$ is a twice continuously differentiable function. Given a time horizon $\mathbb{T}$, the safe exit controllers synthesis problem is to synthesize a locally Lipschitz controller $\boldsymbol{u}(\cdot) : \overline{\mathcal{C}} \to \mathbb{R}^m$ of maximizing lower bounds of the exit probability, i.e., solving the following optimization:

$$\begin{aligned} &\max_{\boldsymbol{u}} p_{\boldsymbol{x}_0} \\ &\text{s.t. } \mathbb{P}\left(\left\{\boldsymbol{w} \in \Omega \mid \begin{matrix} \exists t \in \mathbb{T}. g(\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t)) = 1 \wedge \\ \forall \tau \in [0,t). \boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(\tau) \in \mathcal{C} \end{matrix} \right\}\right) \geq p_{\boldsymbol{x}_0}, \end{aligned} \quad (4)$$

where $\mathbb{T} = [0,T]$ if $T < \infty$, and $\mathbb{T} = [0,\infty)$ otherwise.

III. Exit Controllers Synthesis

In this section, we describe our approach to solving the safe exit controllers synthesis problems I and II. We first focus on Problem I in Subsection III-A, where we present a condition that exit controllers satisfy in order to derive lower bounds on the exit probabilities for both infinite and finite time horizons. This condition involves two free parameters (i.e., a and b) that need to be optimized. Then, we extend this condition to Problem II in Subsection III-B. Finally, in Subsection III-C, we construct linear programs to online synthesize optimal exit controllers implicitly for both Problems I and II. By optimizing the two free parameters a and b from the conditions, we design exit controllers online that maximize the lower bounds on the exit probabilities.

A. Safe Exit Controllers Synthesis Conditions for Problem I

This subsection introduces a condition that exit controllers satisfy in order to derive lower bounds on the exit probabilities in Problem I for both infinite and finite time horizons.

The construction of the condition lies on an auxiliary stochastic process $\{\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t), t \in \mathbb{R}_{\geq 0}\}$ for $\boldsymbol{x}_0 \in \overline{\mathcal{C}}$ that is a stopped process corresponding to $\{\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t), t \in [0, T^{\boldsymbol{x}_0}(\boldsymbol{w}))\}$ and the set $\mathcal{C}$, i.e.,

$$\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t) = \begin{cases} \boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t) & \text{if } t < \tau^{\boldsymbol{x}_0}(\boldsymbol{w}) \\ \boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(\tau^{\boldsymbol{x}_0}(\boldsymbol{w})) & \text{if } t \geq \tau^{\boldsymbol{x}_0}(\boldsymbol{w}) \end{cases}, \quad (5)$$

where

$$\tau^{\boldsymbol{x}_0}(\boldsymbol{w}) = \inf\{t \mid \boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t) \in \partial\mathcal{C}\}$$

is the first time of exit of $\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t)$ from the open set $\mathcal{C}$. It is worth remarking here that if the path $\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t)$ escapes to infinity in finite time, it must touch the boundary of the set $\mathcal{C}$ and thus $\tau^{\boldsymbol{x}_0}(\boldsymbol{w}) \leq T^{\boldsymbol{x}_0}(\boldsymbol{w})$. The stopped process $\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t)$ inherits the right continuity and strong Markovian property of $\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t)$. Moreover, the infinitesimal generator corresponding to $\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t)$ is identical to the one corresponding to $\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t)$ over $\mathcal{X}$, and is equal to zero on the boundary $\partial\mathcal{C}$ [19]. That is, for $v(\boldsymbol{x})$ being a twice continuously differentiable function,

$$\begin{aligned} \widetilde{\mathcal{L}}_{v,\boldsymbol{u}}(\boldsymbol{x}) = \mathcal{L}_{v,\boldsymbol{u}}(\boldsymbol{x}) = &\frac{\partial v}{\partial \boldsymbol{x}}(\boldsymbol{f}_1(\boldsymbol{x}) + \boldsymbol{f}_2(\boldsymbol{x})\boldsymbol{u}(\boldsymbol{x})) \\ &+ \frac{1}{2}\mathbf{tr}(\boldsymbol{\sigma}(\boldsymbol{x})^\top \frac{\partial^2 v}{\partial \boldsymbol{x}^2}\boldsymbol{\sigma}(\boldsymbol{x})) \end{aligned}$$

for $\boldsymbol{x} \in \mathcal{C}$ and $\widetilde{\mathcal{L}}_{v,\boldsymbol{u}}(\boldsymbol{x}) = 0$ for $\boldsymbol{x} \in \partial\mathcal{C}$.

The probability of reaching the set $\mathcal{C}_1$ within the time horizon $\mathbb{T} = [0, T]$ for system (1) while staying inside the set $\mathcal{C}$ before the first time of hitting $\mathcal{C}_1$, is equal to the probability of reaching the set $\mathcal{C}_1$ at the time instant T for the auxiliary stochastic process, where $\mathcal{C}_1 = \{\boldsymbol{x} \in \mathbb{R}^n \mid h(\boldsymbol{x}) = 1\}$.

Lemma 1: Given a time instant $T > 0$ and $\boldsymbol{x}_0 \in \mathcal{C}$,

$$\begin{aligned}&\mathbb{P}(\exists t \in [0,T].\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t) \in \mathcal{C}_1 \wedge \forall \tau \in [0,t).\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(\tau) \in \mathcal{C})\\ &= \mathbb{P}(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(T) \in \mathcal{C}_1) = \mathbb{E}[1_{\mathcal{C}_1}(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(T))].\end{aligned}$$

Moreover, for any $0 < T_1 \leq T_2$,

$$\mathbb{P}(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(T_1) \in \mathcal{C}_1) \leq \mathbb{P}(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(T_2) \in \mathcal{C}_1),$$

where $\mathcal{C}_1 = \{\boldsymbol{x} \in \mathbb{R}^n \mid h(\boldsymbol{x}) = 1\}$.

Proof: It is easy to observe that $\{\boldsymbol{w} \in \Omega \mid \exists t \in [0,T].\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t) \in \mathcal{C}_1 \wedge \forall \tau \in [0,t).\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(\tau) \in \mathcal{C}\} = \{\boldsymbol{w} \in \Omega \mid \widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(T) \in \mathcal{C}_1\}$. Therefore, the conclusion holds.

In addition, we observe that for $T_1 \leq T_2$,

$$\{\boldsymbol{w} \in \Omega \mid \widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(T_1) \in \mathcal{C}_1\} \subseteq \{\boldsymbol{w} \in \Omega \mid \widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(T_2) \in \mathcal{C}_1\}.$$

Consequently, $\mathbb{P}(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(T_1) \in \mathcal{C}_1) \leq \mathbb{P}(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(T_2) \in \mathcal{C}_1)$ holds for $T_1 \leq T_2$. ∎

Remark 1: The conclusion that

$$\begin{aligned}&\mathbb{P}(\exists t \in [0,\infty).\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t) \in \mathcal{C}_1 \wedge \forall \tau \in [0,t).\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(\tau) \in \mathcal{C})\\ &= \lim_{t\to\infty} \mathbb{P}(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t) \in \mathcal{C}_1)\end{aligned}$$

is shown in [17], where $\boldsymbol{x}_0 \in \mathcal{C}$.

Based on the auxiliary stochastic process defined above, a condition can be straightforwardly obtained from Proposition 3 in [18] to lower-bound the exit probability over the infinite time horizon.

Lemma 2: If there exists a locally Lipschitz controller $\boldsymbol{u}(\cdot) : \overline{\mathcal{C}} \to \mathcal{U}$ satisfying the following condition:

$$\mathcal{L}_{h,\boldsymbol{u}}(\boldsymbol{x}) \geq ah(\boldsymbol{x}), \forall \boldsymbol{x} \in \mathcal{C}, \tag{6}$$

where $a > 0$, then

$$\mathbb{P}(\exists t \geq 0.h(\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t)) = 1 \wedge \forall \tau \in [0,t).\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(\tau) \in \mathcal{C}) \geq h(\boldsymbol{x}_0).$$

Lemma 2 introduces a useful condition that includes a free parameter a. This condition is designed to establish a lower bound on the exit probability for Problem I over an infinite time horizon. However, the lower bound provided by Lemma 2 is solely determined by the initial state of the system described in Equation (1), and it does not rely on the value of a. Therefore, optimizing the value of a does not impact the lower bound on the exit probability for Problem I over the infinite time horizon. Moreover, condition (6) may be overly stringent, significantly constraining the feasible space for the controller $\boldsymbol{u}(\cdot) : \overline{\mathcal{C}} \to \mathcal{U}$. Below, we will introduce an additional parameter b into condition (6) to establish a more general and less restrictive condition that can provide lower bounds on exit probabilities for both finite and infinite time horizons in Problem I.

Theorem 1: If there exists a locally Lipschitz controller $\boldsymbol{u}(\cdot) : \overline{\mathcal{C}} \to \mathcal{U}$ satisfying the following condition:

$$\begin{cases}\mathcal{L}_{h,\boldsymbol{u}}(\boldsymbol{x}) \geq ah(\boldsymbol{x}) - b & \forall \boldsymbol{x} \in \mathcal{C}\\ a > b \geq 0\end{cases}, \tag{7}$$

then

$$\mathbb{P}_T \geq \max\{0, \frac{e^{aT}(h(\boldsymbol{x}_0) - \frac{b}{a}) + \frac{b}{a} - 1}{(1 - \frac{b}{a})(e^{aT} - 1)}\}$$

and

$$\mathbb{P}_\infty \geq \max\{0, \frac{h(\boldsymbol{x}_0) - \frac{b}{a}}{1 - \frac{b}{a}}\},$$

where $\mathbb{P}_T = \mathbb{P}(\exists t \in [0,T].h(\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t)) = 1 \wedge \forall \tau \in [0,t).\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(\tau) \in \mathcal{C})$ and $\mathbb{P}_\infty = \mathbb{P}(\exists t \geq 0.h(\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t)) = 1 \wedge \forall \tau \in [0,t).\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(\tau) \in \mathcal{C})$.

Proof: According to (7), we have

$$\begin{cases}\widetilde{\mathcal{L}}_{h,\boldsymbol{u}}(\boldsymbol{x}) + (a-b)1_{\mathcal{C}_1}(\boldsymbol{x}) \geq ah(\boldsymbol{x}) - b & \forall \boldsymbol{x} \in \overline{\mathcal{C}}\\ a > b \geq 0\end{cases}, \tag{8}$$

where $\mathcal{C}_1 = \{\boldsymbol{x} \in \mathbb{R}^n \mid h(\boldsymbol{x}) = 1\}$ and

$$\widetilde{\mathcal{L}}_{h,\boldsymbol{u}}(\boldsymbol{x}) = \begin{cases}\mathcal{L}_{v,\boldsymbol{u}}(\boldsymbol{x}) & \text{if } \boldsymbol{x} \in \mathcal{C}\\ 0 & \text{if } \boldsymbol{x} \in \partial\mathcal{C}\end{cases}.$$

Consequently,

$$\begin{aligned}\mathbb{E}[h(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(T))] &\geq \int_0^T a\mathbb{E}[h(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t))]dt + h(\boldsymbol{x}_0)\\ &- \int_0^T bdt - \int_0^T (a-b)\mathbb{E}[1_{\mathcal{C}_1}(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t))]dt, \forall \boldsymbol{x}_0 \in \mathcal{C}.\end{aligned}$$

Taking $\overline{h}(\boldsymbol{x}) = -h(\boldsymbol{x})$ over $\boldsymbol{x} \in \overline{\mathcal{C}}$, we have

$$\begin{aligned}\mathbb{E}[\overline{h}(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(T))] &\leq \int_0^T a\mathbb{E}[\overline{h}(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t))]dt + \overline{h}(\boldsymbol{x}_0)\\ &+ \int_0^T bdt + \int_0^T (a-b)\mathbb{E}[1_{\mathcal{C}_1}(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t))]dt.\end{aligned}$$

According to Grönwall inequality in the integral form, we further have

$$\begin{aligned}&\mathbb{E}[\overline{h}(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(T))] \leq \alpha(T) + \int_0^T \alpha(s)ae^{a(T-s)}ds\\ &= \overline{h}(\boldsymbol{x}_0) + \int_0^T \overline{h}(\boldsymbol{x}_0)ae^{a(T-s)}ds + bT + \int_0^T bsae^{a(T-s)}ds\\ &\quad + (a-b)\int_0^T \mathbb{E}[1_{\mathcal{C}_1}(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(s))]ds\\ &\quad + a(a-b)\int_0^T \int_0^s \mathbb{E}[1_{\mathcal{C}_1}(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t))]dte^{a(T-s)}ds\\ &\leq \overline{h}(\boldsymbol{x}_0)e^{aT} - \frac{b}{a} + \frac{b}{a}e^{aT}\\ &\quad + (a-b)e^{aT}\mathbb{P}(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(T) \in \mathcal{C}_1)(-\frac{1}{a}e^{-aT} + \frac{1}{a})\end{aligned}$$

where $\alpha(s) = \overline{h}(\boldsymbol{x}_0) + \int_0^s (a-b)\mathbb{E}[1_{\mathcal{C}_1}(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t))]dt + \int_0^s bdt$. The last inequality is obtained according to Lemma 1.

Thus,

$$\begin{aligned}-1 \leq \mathbb{E}[\overline{h}(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(T))] &\leq \overline{h}(\boldsymbol{x}_0)e^{aT} - \frac{b}{a} + \frac{b}{a}e^{aT}\\ &+ (a-b)e^{aT}\mathbb{P}(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(T) \in \mathcal{C}_1)(-\frac{1}{a}e^{-aT} + \frac{1}{a})\end{aligned}$$

After rearrangement, we have the conclusion that $\mathbb{P}(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(T) \in \mathcal{C}_1) \geq \max\{0, \frac{e^{aT}(h(\boldsymbol{x}_0) - \frac{b}{a}) + \frac{b}{a} - 1}{(1 - \frac{b}{a})(e^{aT} - 1)}\}$.

Furthermore, according to Lemma 1, $\mathbb{P}_{\mathbb{T}} \geq \max\{0, \frac{e^{aT}(h(\boldsymbol{x}_0)-\frac{b}{a})+\frac{b}{a}-1}{(1-\frac{b}{a})(e^{aT}-1)}\}$.

That $\mathbb{P}_{\infty} \geq \max\{0, \frac{h(\boldsymbol{x}_0)-\frac{b}{a}}{1-\frac{b}{a}}\}$ can be obtained via letting T approach infinity in $\frac{e^{aT}(h(\boldsymbol{x}_0)-\frac{b}{a})+\frac{b}{a}-1}{(1-\frac{b}{a})(e^{aT}-1)}$. ∎

The reason that b is not allowed to be less than zero in Theorem 1 lies in (8), since the contradiction that $0 \geq -b$ will be obtained over $\{\boldsymbol{x} \in \mathbb{R}^n \mid h(\boldsymbol{x}) = 0\}$ if $b \leq 0$.

B. Safe Exit Controllers Synthesis Conditions for Problem II

This subsection introduces a condition to derive lower bounds on the exit probabilities in Problem II for both infinite and finite time horizons.

The condition introduced is an extension of the one (7) in Theorem 1. Furthermore, in Problem I, leaving the set $\mathcal{C}$ for system (1) is guaranteed when it hits certain part of its boundary, i.e., $\mathcal{C}_1$. However, in the extended condition, hitting any state in the boundary of the set $\mathcal{C}$ implies that system (1) will leave the set $\mathcal{C}$. To accommodate this situation, the free parameter b in the extended condition is allowed to be smaller than zero. This flexibility allows for a wider range of scenarios to be considered, expanding the feasibility of the condition and providing more general lower bounds on exit probabilities.

Theorem 2: Given a safe but uncomfortable set $\mathcal{C}$ defined in Section II, if there exists a locally Lipschitz controller $\boldsymbol{u}(\cdot) : \overline{\mathcal{C}} \to \mathcal{U}$ satisfying the following condition:

$$\begin{cases} \mathcal{L}_{g,\boldsymbol{u}}(\boldsymbol{x}) \geq a g(\boldsymbol{x}) - b \quad \forall \boldsymbol{x} \in \mathcal{C} \\ a > b \end{cases}, \tag{9}$$

then for $\boldsymbol{x}_0 \in \mathcal{C}$,

1) when $a > 0$,

$$\mathbb{P}(\exists t \in [0,T]. \boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t) \in \partial\mathcal{C}) \geq \max\{0, \frac{e^{aT}(g(\boldsymbol{x}_0)-\frac{b}{a})+\frac{b}{a}-1}{(1-\frac{b}{a})(e^{aT}-1)}\}$$

and

$$\mathbb{P}(\exists t \in [0,\infty). \boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t) \in \partial\mathcal{C}) \geq \max\{0, \frac{g(\boldsymbol{x}_0)-\frac{b}{a}}{1-\frac{b}{a}}\}.$$

2) when $a \leq 0$,

$$\mathbb{P}(\exists t \in [0,T]. \boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t) \in \partial\mathcal{C}) \geq \max\{0, 1-\frac{g(\boldsymbol{x}_0)-1}{(b-a)T}\}$$

and $\mathbb{P}(\exists t \in [0,\infty). \boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t) \in \partial\mathcal{C}) = 1$.

Proof: 1). The conclusion for $a > 0$ can be obtained by following the proof in Theorem 1, with $\mathcal{C}_1$ being replaced by $\partial\mathcal{C}$.

2). Since $g(\boldsymbol{x})$ satisfies $g(\boldsymbol{x}) \leq 1$ over $\overline{\mathcal{C}}$, we have $ag(\boldsymbol{x}) - b \geq (a-b) > 0$. Therefore,

$$\widetilde{\mathcal{L}}_{g,\boldsymbol{u}}(\boldsymbol{x}) + (a-b)1_{\partial\mathcal{C}}(\boldsymbol{x}) \geq a - b \geq 0, \forall \boldsymbol{x} \in \overline{\mathcal{C}}.$$

Further, we conclude that

$$\mathbb{E}[g(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t))] \geq g(\boldsymbol{x}_0), \forall t \in [0,T]$$

and

$$\mathbb{E}[g(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(T))] - g(\boldsymbol{x}_0) + (a-b)\int_0^T \mathbb{E}[1_{\partial\mathcal{C}}(\widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t))]dt \geq (a-b)T.$$

According to Lemma 1, we further have

$$(a-b)T\mathbb{P}(\exists t \in [0,T]. \widetilde{\boldsymbol{\phi}}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t) \in \partial\mathcal{C}) \geq (a-b)T + g(\boldsymbol{x}_0) - 1,$$

which implies $\mathbb{P}(\exists t \in [0,T]. \boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t) \in \partial\mathcal{C}) \geq 1 - \frac{g(\boldsymbol{x}_0)-1}{(b-a)T}$. Thus, we have

$$\mathbb{P}(\exists t \in [0,T]. \boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t) \in \partial\mathcal{C}) \geq \max\{0, 1-\frac{g(\boldsymbol{x}_0)-1}{(b-a)T}\}.$$

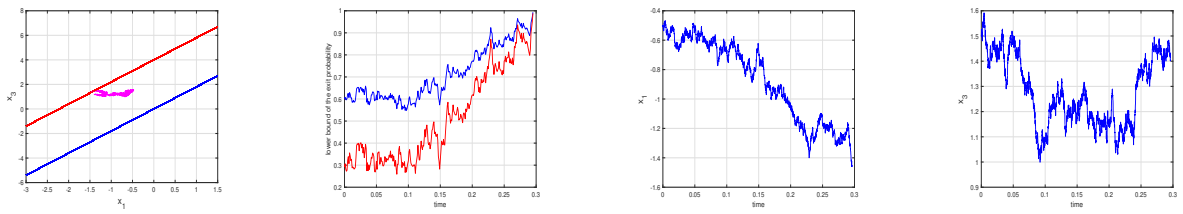
Via letting T approach infinity, we further have $\mathbb{P}(\exists t \in [0,\infty). \boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(t) \in \partial\mathcal{C}) = 1$. ∎

C. Linear-Program-Based Controllers

In this subsection, we introduce our online linear programming based method for implicitly synthesizing optimal exit controllers that maximize lower bounds of exit probabilities for both Problems I and II.

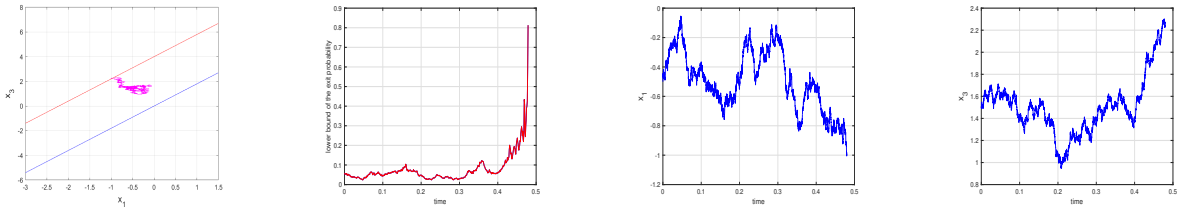
Except for the controller $\boldsymbol{u}$, both conditions (7) and (9) involve two additional free parameters, a and b, that need to be determined in order to optimize the lower bounds stated in Theorem 1 and 2. These conditions have a linear dependency on these parameters. However, the lower bounds exhibit nonlinearity with respect to a and b, except when $a \leq 0$ and $T \to \infty$ in Theorem 2. Hence, it is not advisable to solve a maximization problem with condition (7) (or (9)) and the lower bounds from Theorem 1 (or 2) as the objective function, especially for online optimization which demands high efficiency.

On the other hand, it is observed that both the lower bounds $\frac{e^{aT}(h(\boldsymbol{x}_0)-\frac{b}{a})+\frac{b}{a}-1}{(1-\frac{b}{a})(e^{aT}-1)}$ and $\frac{h(\boldsymbol{x}_0)-\frac{b}{a}}{1-\frac{b}{a}}$ in Theorem 1 are monotonically increasing with a and decreasing with b. Similar to Theorem 1, all the lower bounds, i.e., $\frac{e^{aT}(g(\boldsymbol{x}_0)-\frac{b}{a})+\frac{b}{a}-1}{(1-\frac{b}{a})(e^{aT}-1)}$, $\frac{g(\boldsymbol{x}_0)-\frac{b}{a}}{1-\frac{b}{a}}$, $1-\frac{g(\boldsymbol{x}_0)-1}{(b-a)T}$, and 1, in Theorem 1 are monotonically increasing with respect to a and decreasing with respect to b. Moreover, it is observed that as the value of a tends towards zero from the right, the lower bound $\frac{e^{aT}(g(\boldsymbol{x}_0)-\frac{b}{a})+\frac{b}{a}-1}{(1-\frac{b}{a})(e^{aT}-1)}$ in Theorem 2 tends to approach $1-\frac{g(\boldsymbol{x}_0)-1}{bT}$, i.e., $\lim_{a\to 0^+} \frac{e^{aT}(g(\boldsymbol{x}_0)-\frac{b}{a})+\frac{b}{a}-1}{(1-\frac{b}{a})(e^{aT}-1)} = 1-\frac{g(\boldsymbol{x}_0)-1}{bT}$, which is equal to the lower bound in the case of $a \leq 0$ with $a = 0$. Thus, the objective function $\max(a - wb)$ is a suitable candidate, where w denotes a specified weighting factor. This factor allows for the adjustment of the relative importance of b compared to a according to the specific requirements of the problem. Additionally, in order to ensure boundedness of $a - wb$, we impose a bound constraint on a and b. Consequently, we can synthesize exit controllers of maximizing lower bounds of the exit probabilities for Problem I online in the form of point-wise optimization as



a-1 a-2 a-3 a-4

(a) $w = 10^{12}$



b-1 b-2 b-3 b-4

(b) $w = 1$

Fig. 1: Illustration of trajectories and lower bounds of exit probabilities computed via solving optimization (10) online. (a-1 and b-1: red line – $\mathcal{C}_1 = \{(x_1, x_3)^\top \mid \frac{x_3 - 1.8x_1}{4} = 1\}$, blue line – $\{(x_1, x_3)^\top \mid \frac{x_3 - 1.8x_1}{4} = 0\}$, magenta curve – trajectory driven by the controller computed via solving (10); a-2 and b-2: red curve – lower bound of the exit probability when $\mathbb{T} = [0, 2]$ with respect to time, i.e., $\frac{e^{a(T-t)}(h(\boldsymbol{x}(t)) - \frac{b}{a}) + \frac{b}{a} - 1}{(1 - \frac{b}{a})(e^{a(T-t)} - 1)}$, blue curve – lower bound of the exit probability when $\mathbb{T} = [0, \infty)$ with respect to time (blue and red curves collide in b-2), i.e., $\frac{h(\boldsymbol{x}(t)) - \frac{b}{a}}{1 - \frac{b}{a}}$; a-3 and b-3: $x_1(t)$; a-4 and b-4: $x_3(t)$.)

in [12] using linear programs below.

$$\begin{aligned} \max_{\boldsymbol{u}(\boldsymbol{x}) \in \mathcal{U}, a, b} \; & a - wb \\ \text{s.t. } & \mathcal{L}_{h,\boldsymbol{u}}(\boldsymbol{x}) \geq ah(\boldsymbol{x}) - b, \\ & a > b \geq 0 \\ & a \leq \delta \end{aligned} \tag{10}$$

where $\mathcal{L}_{h,\boldsymbol{u}}(\boldsymbol{x}) = \frac{\partial h}{\partial \boldsymbol{x}}(\boldsymbol{f}_1(\boldsymbol{x}) + \boldsymbol{f}_2(\boldsymbol{x})\boldsymbol{u}(\boldsymbol{x})) + \frac{1}{2}\mathbf{tr}(\boldsymbol{\sigma}(\boldsymbol{x})^\top \frac{\partial^2 h}{\partial \boldsymbol{x}^2}\boldsymbol{\sigma}(\boldsymbol{x}))$ and $\delta > 0$ is a specified bound.

Correspondingly, we can synthesize exit controllers of maximizing lower bounds of the exit probabilities for Problem II online in the form of point-wise optimization using linear programs below.

$$\begin{aligned} \max_{\boldsymbol{u}(\boldsymbol{x}) \in \mathcal{U}, a, b} \; & a - wb \\ \text{s.t. } & \mathcal{L}_{g,\boldsymbol{u}}(\boldsymbol{x}) \geq ag(\boldsymbol{x}) - b, \\ & a > b \\ & a, b \in [-\delta, \delta] \end{aligned} \tag{11}$$

where $\mathcal{L}_{g,\boldsymbol{u}}(\boldsymbol{x}) = \frac{\partial g}{\partial \boldsymbol{x}}(\boldsymbol{f}_1(\boldsymbol{x}) + \boldsymbol{f}_2(\boldsymbol{x})\boldsymbol{u}(\boldsymbol{x})) + \frac{1}{2}\mathbf{tr}(\boldsymbol{\sigma}(\boldsymbol{x})^\top \frac{\partial^2 g}{\partial \boldsymbol{x}^2}\boldsymbol{\sigma}(\boldsymbol{x}))$ and $\delta > 0$ is a specified bound.

It is worth noting that due to the imposed constraint on the control input, specifically $u \in \mathcal{U}$, the existence of a solution for either of the optimization problems (10) and (11) is not guaranteed, even if the boundedness requirements on a and b are disregarded. *However, as in [12], this issue can be resolved by incorporating slack variables into* $\mathcal{L}_{h,u}(x) \geq ah(x) - b$ *in* (10) *and* $\mathcal{L}_{g,u}(x) \geq ag(x) - b$ *in* (11).

IV. Examples

In this section we demonstrate our linear-programming based exit controllers synthesis method on one example involving three scenarios.

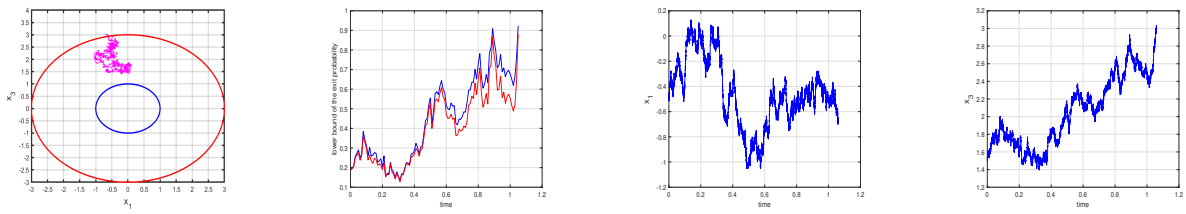
Consider a system with three states $(x_1, x_2, x_3)^\top$[13], [20], where x_1 denotes the velocity of the following vehicle, x_2 denotes the velocity of the leading vehicle, and x_3 denotes the distance between the vehicles. The velocity of the leading vehicle was chosen as a constant. The input is the force applied to the following vehicle, leading to dynamics

$$d\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} -F_r(\boldsymbol{x})/M \\ 0 \\ x_2 - x_1 \end{pmatrix} + \begin{pmatrix} 1/M \\ 0 \\ 0 \end{pmatrix} \boldsymbol{u} + \sum dW,$$

where $F_r = f_0 + f_1 x_1 + f_2 x_1^2$ is the aerodynamic drag with constants $f_0 = 0.1, f_1 = 5$, and $f_2 = 0.25$. The mass $M = 1650$, $\sum = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, and $u \in [-1, 1]$. The initial state for x_2 was chosen as $x_2(0) = 0.5$. Since the velocity of the leading vehicle was chosen as a constant, the system is equivalently reduced to

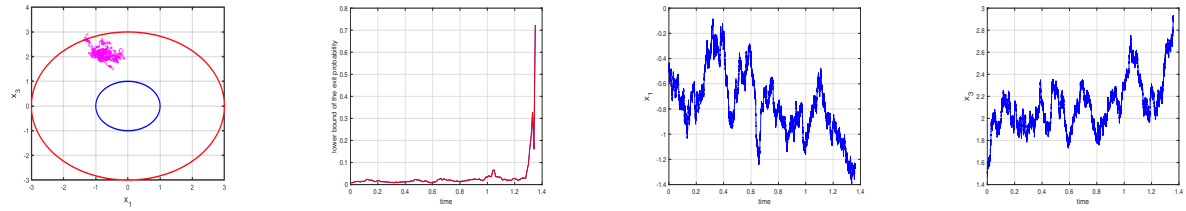
$$d\begin{pmatrix} x_1 \\ x_3 \end{pmatrix} = \begin{pmatrix} -F_r(\boldsymbol{x})/M \\ 0.5 - x_1 \end{pmatrix} + \begin{pmatrix} 1/M \\ 0 \end{pmatrix} \boldsymbol{u} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} dW.$$

We consider three scenarios with both the finite time horizon of $\mathbb{T} = [0, 2]$ and the infinite time horizon of $\mathbb{T} =$



a-1 a-2 a-3 a-4

(a) $w = 10^{12}$



b-1 b-2 b-3 b-4

(b) $w = 1$

Fig. 2: Illustration of trajectories and lower bounds of exit probabilities computed via solving optimization (10) online. (a-1 and b-1: red line – $\mathcal{C}_1 = \{(x_1, x_3)^\top \mid \frac{x_1^2+x_3^2-1}{8} = 1\}$, blue line – $\{(x_1, x_3)^\top \mid \frac{x_1^2+x_3^2-1}{8} = 0\}$, magenta curve – trajectory driven by the controller computed via solving (10); a-2 and b-2: red curve – lower bound of the exit probability when $\mathbb{T} = [0, 2]$ with respect to time, i.e., $\frac{e^{a(T-t)}(h(\boldsymbol{x}(t))-\frac{b}{a})+\frac{b}{a}-1}{(1-\frac{b}{a})(e^{a(T-t)}-1)}$, blue curve – lower bound of the exit probability when $\mathbb{T} = [0, \infty)$ with respect to time (blue and red curves collide in b-2), i.e., $\frac{h(\boldsymbol{x}(t))-\frac{b}{a}}{1-\frac{b}{a}}$; a-3 and b-3: $x_1(t)$; a-4 and b-4: $x_3(t)$.)

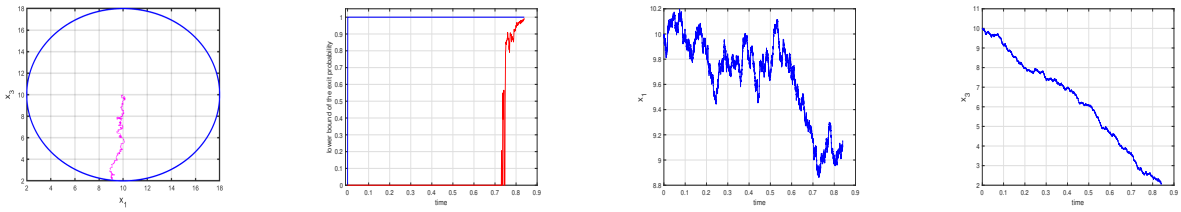
$[0, \infty)$. Moreover, the weighting factor w in the optimization problems (10) and (11) is chosen to be 10^{12} and 1. The first two scenarios correspond to Problem I. The first scenario features an unbounded safe set $\mathcal{S}$ and uncomfortable set $\mathcal{C}$, while the second one features an unbounded safe set $\mathcal{S}$ but a bounded uncomfortable set $\mathcal{C}$. The third scenario corresponds to Problem II, which includes a bounded uncomfortable set $\mathcal{C}$. Detailed configuration information and some computation results are presented below.

1) The safe set is $\mathcal{S} = \{(x_1, x_3)^\top \mid x_3 - 1.8x_1 > 0\}$, the safe but uncomfortable set is defined as $\mathcal{C} = \{(x_1, x_3)^\top \mid 0 < \frac{x_3-1.8x_1}{4} < 1\}$, and the initial state is set to $(-0.5, 1.5)^\top$. The simulation trajectories and lower bounds of exit probabilities, computed by solving the linear optimization (10) with $\delta = 10$, are presented in Fig. 1.
2) The safe set is $\mathcal{S} = \{(x_1, x_3)^\top \mid x_1^2 + x_3^2 - 1 > 0\}$, the safe but uncomfortable set is $\mathcal{C} = \{(x_1, x_3)^\top \mid 0 < \frac{x_1^2+x_3^2-1}{8} < 1\}$, and the initial state is $(-0.5, 1.5)^\top$. The simulation trajectories and lower bounds of exit probabilities, computed by solving the linear optimization (10) with $\delta = 10$, are presented in Fig. 2.
3) The safe set is $\mathcal{S} = \{(x_1, x_3)^\top \mid x_1^2 + x_3^2 > 1\}$, the uncomfortable set is $\mathcal{C} = \{(x_1, x_3)^\top \mid \frac{(x_1-10)^2+(x_3-10)^2}{64} < 1\}$, and the initial state is $(10, 10)^\top$. The simulation trajectories and lower bounds of exit probabilities, computed by solving optimization (11) with $\delta = 10$, are presented in Fig. 3.

The results presented in Figures 1, 2, and 3 demonstrate the significant impact of the weighting factor w on the performance of the synthesized controllers. Notably, in the first two scenarios, the controllers computed with $w = 10^{12}$ show superior performance in safely guiding the system out of the uncomfortable set $\mathcal{C}$ with high probabilities, compared to those obtained with $w = 1$, especially during the initial phase. In the third scenario, where $\partial\mathcal{C} \cap \partial\mathcal{S} = \emptyset$, the controller synthesized with $w = 10^{12}$ exhibits superior performance in terms of achieving high probabilities for safely driving the system out of the uncomfortable set $\mathcal{C}$, when an infinite time horizon $\mathbb{T} = [0, \infty)$ is considered. However, the performance during the initial phase is inferior when the time horizon is limited to $\mathbb{T} = [0, 2]$, compared to that obtained with $w = 1$.

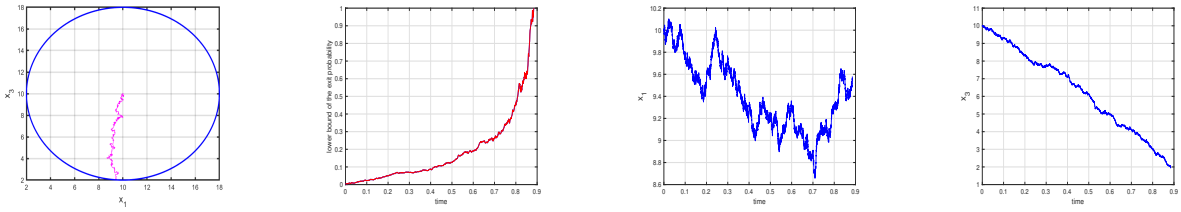
V. Conclusion

This paper focused on the synthesis of safe exit controllers for continuous-time systems described by SDEs. The main objective is to design controllers that maximize the lower bounds of the exit probability that the system escapes from a safe but uncomfortable set within a specific time horizon and enters a comfortable set. The paper discussed two cases: the first case involves the scenario where the boundary of the safe set is a subset of the boundary of the safe but uncomfortable set, and the second case deals with situations where the boundaries do not intersect. In the first case, the paper presented a sufficient condition for lower-bounding the exit probability. This condition provides a guideline for constructing online linear programming problems, which in turn facilitate synthesizing optimal exit controllers implicitly.



a-1 a-2 a-3 a-4

(a) $w = 10^{12}$



b-1 b-2 b-3 b-4

(b) $w = 1$

Fig. 3: Illustration of trajectories and lower bounds of exit probabilities computed via solving optimization (11) online. (a-1 and b-1: blue curve – $\{(x_1, x_3)^\top \mid \frac{(x_1-1)^2+(x_3-10)^2}{64} = 1\}$, magenta curve – trajectory driven by the controller computed via solving (11); a-2 and b-2: red curve – lower bound of the exit probability when $\mathbb{T} = [0, 2]$ with respect to time, i.e., $\frac{e^{a(T-t)}(g(\boldsymbol{x}(t))-\frac{b}{a})+\frac{b}{a}-1}{(1-\frac{b}{a})(e^{a(T-t)}-1)}$ if $a > 0$ and $1 - \frac{g(\boldsymbol{x}(t))-1}{(b-a)(T-t)}$ if $a \leq 0$, blue curve – lower bound of the exit probability when $\mathbb{T} = [0, \infty)$ with respect to time (blue and red curves collide in b-2), i.e., $\frac{h(\boldsymbol{x}(t))-\frac{b}{a}}{1-\frac{b}{a}}$ if $a > 0$ and 1 if $a \leq 0$; a-3 and b-3: $x_1(t)$; a-4 and b-4: $x_3(t)$.)

These controllers are designed to maximize the lower bounds of the exit probabilities. Then, this sufficient condition was extended to the second case, where the boundaries of the safe set and the uncomfortable set do not intersect. Finally, an example was presented to validate the proposed method.

The first case discussed in this paper involves a scenario where the boundary of the safe set intersects with that of the uncomfortable set. However, it is limited to the typical case where the boundary of the safe set is a subset of the boundary of the uncomfortable set. In future studies, we will explore more general cases where only a subset of the safe set's boundary intersects that of the uncomfortable set.

REFERENCES

[1] Peter E Kloeden, Eckhard Platen, Peter E Kloeden, and Eckhard Platen. *Stochastic differential equations*. Springer, 1992.

[2] Martin Fränzle, Ernst Moritz Hahn, Holger Hermanns, Nicolás Wolovick, and Lijun Zhang. Measurability and safety verification for stochastic hybrid systems. In *Proceedings of the 14th international conference on Hybrid systems: computation and control*, pages 43–52, 2011.

[3] Claire J Tomlin, Ian Mitchell, Alexandre M Bayen, and Meeko Oishi. Computational techniques for the verification of hybrid systems. *Proceedings of the IEEE*, 91(7):986–1001, 2003.

[4] Alessandro Abate, Joost-Pieter Katoen, John Lygeros, and Maria Prandini. Approximate model checking of stochastic hybrid systems. *European Journal of Control*, 16(6):624–641, 2010.

[5] Stephen Prajna, Ali Jadbabaie, and George J Pappas. A framework for worst-case and stochastic safety verification using barrier certificates. *IEEE Transactions on Automatic Control*, 52(8):1415–1428, 2007.

[6] Jean Ville. Etude critique de la notion de collectif. 1939.

[7] Jacob Steinhardt and Russ Tedrake. Finite-time regional verification of stochastic non-linear systems. *The International Journal of Robotics Research*, 31(7):901–923, 2012.

[8] Harold Joseph Kushner and Kushner. *Stochastic stability and control*, volume 33. Academic press New York, 1967.

[9] Cesar Santoyo, Maxence Dutreix, and Samuel Coogan. A barrier function approach to finite-time stochastic system verification and control. *Automatica*, 125:109439, 2021.

[10] Petter Nilsson and Aaron D Ames. Lyapunov-like conditions for tight exit probability bounds through comparison theorems for sdes. In *2020 American Control Conference (ACC)*, pages 5175–5181. IEEE, 2020.

[11] Randy A Freeman and Petar V Kokotovic. Inverse optimality in robust stabilization. *SIAM journal on control and optimization*, 34(4):1365–1391, 1996.

[12] Aaron D Ames, Xiangru Xu, Jessy W Grizzle, and Paulo Tabuada. Control barrier function based quadratic programs for safety critical systems. *IEEE Transactions on Automatic Control*, 62(8):3861–3876, 2016.

[13] Chuanzheng Wang, Yiming Meng, Stephen L Smith, and Jun Liu. Safety-critical control of stochastic systems using stochastic control barrier functions. In *2021 60th IEEE Conference on Decision and Control (CDC)*, pages 5924–5931. IEEE, 2021.

[14] Bai Xue, Renjue Li, Naijun Zhan, and Martin Fränzle. Reach-avoid analysis for stochastic discrete-time systems. In *2021 American Control Conference (ACC)*, pages 4879–4885. IEEE, 2021.

[15] Bai Xue. Reachability verification for stochastic discrete-time dynamical systems. *arXiv preprint arXiv:2302.09843*, 2023.

[16] Yiqing Yu, Taoran Wu, Bican Xia, Ji Wang, and Bai. Xue. Safe probabilistic invariance verification for stochastic discrete-time dynamical systems. In *2023 62nd IEEE Conference on Decision and Control (CDC)*, pages 5175–5181. IEEE, 2023.

[17] Bai Xue, Naijun Zhan, and Martin Fränzle. Reach-avoid analysis for polynomial stochastic differential equations. *IEEE Transactions on Automatic Control*, 69(3):1882–1889, 2024.

[18] Bai Xue. Reach-avoid controllers synthesis for safety critical systems. *To appear in IEEE Transactions on Automatic Control*, 2024.

[19] Harold J Kushner. *Stochastic stability and control*. New York: Academic, 1967.

[20] Andrew Clark. Control barrier functions for complete and incomplete information stochastic systems. In *2019 American Control Conference (ACC)*, pages 2928–2935. IEEE, 2019.