Safety Verification for Random Ordinary Differential Equations

Bai Xue, *Member, IEEE*, Martin Fränzle, Naijun Zhan, Sergiy Bogomolov and Bican Xia

***Abstract*—Random ordinary differential equations (RODEs) are ordinary differential equations (ODEs) that contain a stochastic process in their vector field functions. They have been used for many years in a wide range of applications, but have been a shadow existence to stochastic differential equations (SDEs) despite being able to model a wider and often physically more adequate range of disturbances. In this paper we study the safety verification problem over both finite time horizons and the infinite time horizon for RODEs incorporating Wiener processes. Concretely, we investigate the *p*-safety problem, where we identify the set of initial states from which the probability to satisfy safety specifications is at least *p*. Based on identifying a set of sample paths whose probability measure is larger than *p*, we propose a method of reducing stochastic reachability to adversary reachability of ODEs for solving the *p*-safety problem over finite time horizons. This method permits an efficient lifting of reach-set computation methods for perturbed ODEs to RODEs. In this method the *p*-safety problem over finite time horizons is reduced to the problem of inner-approximating robust backward reachable sets for ODEs with time-varying perturbation inputs. We then extend the method to the *p*-safety problem over the infinite time horizon. Finally, we demonstrate our method on several examples.**

***Index Terms*—Safety Verification, Random Ordinary Differential Equations, Perturbed Ordinary Differential Equations.**

I. Introduction

> Christiaan Huygens, 1673, see [33] "*I believe that we do not know anything for certain, but everything probably.*"

The rapidly increasing deployment of cyber-physical systems into diverse safety-critical application domains ranging from transportation systems to medical systems renders safety verification for these systems important [31]. The safety verification problem is often reduced to a reachability problem, which justifies whether the reach states enter a specified set of unsafe states [12]. However, the exact computation of reachable sets of a nonlinear system is generally impossible. Despite existence of solvable cases [14], reachability analysis usually employs either over-approximations of the exact reach set to prove that a system starting from the initial states satisfies its safety specifications [5], [7], [32], or under-approximations to identify a set of states such that the system starting from them violates specified safety properties [15], [43]–[45].

Ordinary differential equations (ODEs) are often used to model deterministic systems. Consequently, significant research has been invested in reachability analysis of such systems. However, ODEs are often an idealized model in modeling real-world systems, as stochastic processes are often involved in many areas such as physics, engineering, ecology, biology and other disciplines [6]. For example, the motion model of a car cannot be formalized exactly in general if we do not know all the external forces affecting the car and the acts of the driver. In many scenarios the unknown subphenomena can be modeled as stochastic processes, which leads to mathematical models involving stochastic processes. In contrast to the Boolean safety verification of deterministic systems, when considering stochastic systems, i.e., systems involving stochastic processes, the safety notion is relaxed. Usually, the p-safety problem is considered. The stochastic system is p-safe if it respects safety specifications with a probability of at least p, i.e., the probability that the system trajectories satisfy safety specifications is at least p.

In the literature stochastic differential equations (SDEs) are equations that are often used to describe certain stochastic processes. Early work on SDEs was pursued to describe Brownian motion in Einstein's famous paper [10], and at the same time by Smoluchowski [40]. Afterwards, mathematical formulations of Brownian motion were attempted by many mathematicians. Itô derived an SDE of the following form

$$dX(t) = a(t, X(t))dt + \sigma(t, X(t))dW(t),$$

where $W(t)$ denotes a Wiener process which is a Brownian motion. It can be reformulated in the following integral form:

$$\begin{aligned} X(t) =& X(t_0) + \int_{t_0}^{t} a(s, X(s))ds + \\ & \lim_{|\Delta|\to 0} \sum_{i=1}^{n} \sigma(s_{i-1}, X(s_{i-1}))(W(s_i) - W(s_{i-1})) \end{aligned} \tag{1}$$

B. Xue and N. Zhan are with State Key Lab. of Computer Science, Institute of Software, CAS, and University of Chinese Academy of Sciences, Beijing, China email:{xuebai,znj}@ios.ac.cn

M. Fränzle is with the Department of Computing Science, Carl von Ossietzky Universität, Oldenburg, Germany email: martin.fraenzle@uol.de

S. Bogomolov is with School of Computing, Newcastle University, United Kingdom email: sergiy.bogomolov@newcastle.ac.uk

B. Xia is with LMAM & School of Mathematical Sciences, Peking University, Beijing, China email: xbc@math.pku.edu.cn

Manuscript received April 17, 2020; revised June 17, 2020; accepted July 6, 2020. This article was presented in the International Conference on Embedded Software 2020 and appears as part of the ESWEEK-TCAD special issue.

This work has been supported through grants by NSFC under grant No. 61872341, 61836005, 61625206, 61732001, 61532019, the CAS Pioneer Hundred Talents Program under grant No. Y8YC235015, Deutsche Forschungsgemeinschaft through the grants DFG GRK 1765 "System Correctness under Adverse Conditions" and FR 2715/4-1 "Integrated Socio-technical Models for Conflict Resolution and Causal Reasoning", and the Air Force Office of Scientific Research under award number FA2386-17-1-4065. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the United States Air Force.

for $t_0 = s_0 < \ldots < s_n = t$ and $\Delta = \max_{1\leq i\leq n}(s_i - s_{i-1})$ for nonanticipative process $\sigma(t, X(t))$, i.e., independent of the future increments of the Wiener process. For a thorough study of SDEs we refer to the literature [4], [30]. There also exists work on safety verification of systems modelled by SDEs, e.g., [11], [21], [22], [26], [28], [41].

Another important modeling approach to include noise terms in differential equations is random ordinary differential equations (RODEs) [37], which seem to have been long overshadowed by SDEs. SDEs and RODEs are two different models. RODEs are ODEs which have a stochastic process in their vector field functions, while SDEs are not ODEs. Recently, there is evidence that SDEs fail to describe dynamics of certain systems however, RODEs are able to do so. A typical example can be found in [8], which shows that RODE is better than SDE in describing the SIR system. In general, RODEs can be written in the form:

$$\frac{d\boldsymbol{x}}{dt} = \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{Y}(t)), \tag{2}$$

where $\boldsymbol{Y}(t)$ is a stochastic process such as Brownian motion, fractional Brownian motion, and the noise processes with jumps, e.g., a Poisson process or compound Poisson process. In some situations it is considerably easier to develop models with noise in the form of RODEs than it is with SDEs. RODEs have also been used in a wide range of applications such as biology, medicine, population dynamics, and engineering and play an important role in the theory of random dynamical systems [16], [24]. Yet, to the best of our knowledge, there is so far no work on studying safety verification of RODEs with the aforementioned stochastic processes.

In this paper we investigate the safety verification problem over both finite time horizons and the infinite time horizon for systems modeled by RODEs incorporating a Wiener process, which is a widely used random process in engineering, finance, and physical sciences. The proposed method is based on the reduction of stochastic reachability for RODEs to adversarial reachability of ODEs. This method can be straightforwardly extended to RODEs with other types of stochastic processes such as fractional Brownian motions or Poisson processes. Concretely, we attempt to solve the *p*-safety problem, which is to identify the set of p-safe initial states from which the probability to satisfy safety specifications is at least *p*. The safety specification we consider in the case of finite time horizons is a finite-time reach-avoid problem [39], i.e., the requirement of maintaining the system within a specified safe set over the given finite time horizon while entering a target region at the terminal time. When addressing this *p*-safety problem, we first identify a set of sample paths such that its probability measure is larger than *p*, and then by regarding the identified sample paths as perturbation inputs we reduce the *p*-safety problem for RODEs to the problem of inner-approximating robust backward reachable sets for perturbed ODEs. As to the safety verification problem over the infinite time horizon, the safety specification is the requirement of maintaining the system always within a safe set. For solving this problem, by identifying a set of sample paths with probability measure one as perturbation inputs, we first compute a robust invariant set for perturbed ODEs, which is a set of p-safe initial states. Then the method of addressing the p-safety problem over finite time horizons can be used to further expand the set of p-safe initial states by taking the computed robust invariant set as a target set. Several examples are used to illustrate our method.

The main contributions are summarized below:

1). We investigate the safety verification of RODEs with Wiener processes, which appear frequently in practice. To the best of our knowledge, the method in this paper is the first one on safety verification of RODEs with time-varying stochastic processes.

2). We propose a method of reducing stochastic reachability to adversarial reachability of ODEs for safety verification of RODEs, thus permitting the efficient lifting of reach-set computation methods for perturbed ODEs to RODEs with time-varying stochastic processes.

Related Work

Existing literature on safety verification of stochastic systems mainly focuses on stochastic hybrid systems. Stochastic hybrid systems are dynamical systems involving interacting continuous and stochastic dynamics. They arise naturally when modelling embedded systems consisting of components with uncertainty, exhibiting random behavior. The pronounced interest of the research community in safety verification of stochastic hybrid systems has produced a number of different types of stochastic hybrid models and verification methods. The main difference between these classes of stochastic hybrid models lies in the way the stochasticity enters the process [27]. Some models allow SDEs to model continuous evolution [18], [29], while others do not [19], [35]. Some models force transitions to take place from certain states [13], [46], others only allow transitions to take place randomly [42], while some allow both [36]. Also, there are some works on discrete-time stochastic hybrid systems, e.g., [1], whose dynamics are described by difference equations generally. Modeling and verification of more general stochastic hybrid systems are discussed in [41]. However, RODEs do not fall into any existing class of stochastic hybrid systems, thus enriching existing stochastic systems in verification community.

In existing literature only simple kinds of RODEs are investigated with the vector field depending on random time-constant parameters, e.g., [17], [35]. Reachability analysis methods for deterministic systems modeled by ODEs are extended to verify such simple RODEs over finite time horizons. The present paper, however, considers more general RODEs with time-varying stochastic processes such as a Wiener process. By taking the sample paths in stochastic processes as perturbation inputs, our method reduces the p-safety problem for RODEs to the safety verification problem for perturbed ODEs, thereby enabling an efficient lifting of safety verification methods for perturbed ODEs to RODEs.

This paper is structured as follows. In Section II we introduce Wiener processes, RODEs and the p-safety problem. Section III elucidates our approach for solving the *p*-safety problem over both finite time horizons and the infinite time

horizon. After demonstrating our approach on several examples in Section IV, we conclude this paper in Section V.

II. Preliminaries

In this section we first introduce the concept of a Wiener process in Subsection II-A, and then formulate RODEs and the *p*-safety problem in Subsection II-B.

A. Wiener Processes

In this subsection we introduce Wiener processes. Throughout this paper, $\mathcal{C}^k[0,T]$ denotes the space of continuous functions mapping $[0,T]$ into $\mathbb{R}^k$, $\mathcal{C}^k[0,\infty)$ denotes the space of continuous functions for the time interval $[0,\infty)$, and $\mathbb{R}_+$ denotes the set of non-negative values in $\mathbb{R}$. $\mathbb{R}[\cdot]$ denotes the ring of polynomials in variables given by the argument.

Consider a probability space $(\Omega,\mathcal{F},P)$. A family of σ-algebra $\{\mathcal{F}_t, t \geq 0\}$ is called a filtration on this space if $\mathcal{F}_s \subseteq \mathcal{F}_t \subseteq \mathcal{F}$ for $0 \leq s \leq t$. Let $E_{\mathcal{F}_t}$ and $P_{\mathcal{F}_t}$ denote expectation and probability up to the $\sigma-$algebra $\mathcal{F}_t$, respectively. The notion of Wiener processes is formally given:

Definition 1 (Wiener Process)**.** *Let $(\Omega,\mathcal{F},P)$ be a probability space and let $\{\mathcal{F}_t, t \geq 0\}$ be a filtration defined on it. A process $\{W(t,w) : \mathbb{R}_+ \times \Omega \to \mathbb{R}\}$ is called an $\mathcal{F}_t-$Wiener process if it satisfies the following conditions: for $w \in \Omega$,*

1) *$W(0,w) = 0$;*
2) *the increments $W(s,w) - W(t,w)$ are independent of $\mathcal{F}_t$ for every $s \geq t$;*
3) *the increments $W(s,w) - W(t,w)$ are normally distributed with mean 0 and variance $\delta^2(s-t) > 0$ for all $s \geq t \geq 0$; and*
4) *the sample path $W(\cdot,w) : [0,\infty) \to \mathbb{R}$ is in $\mathcal{C}^1[0,\infty)$.*

For the details of the Wiener process we refer the reader to [20]. In Definition 1 we directly define a continuous modification of the Wiener process, which is unique up to indistinguishability due to Kolmogorov's criterion [38].

If $\delta = 1$ in Definition 1, then the process $W(\cdot,\cdot)$ is called a standard $\mathcal{F}_t$-Wiener process. If $\mathcal{F}_t$ simply is a natural filtration, i.e., $\mathcal{F}_t = \sigma(\{W(s,w), 0 \leq s \leq t\})$, then the $\mathcal{F}_t$ prefix is often suppressed and we refer to $W(\cdot,\cdot)$ simply as a Wiener process. It is worth remarking here that $-W(\cdot,\cdot)$ is also a Wiener process.

The reflection principle is one of the most important properties of the Wiener process, which states that the maximum of a Wiener process over the time horizon $[0,t]$ has the same law as the *absolute value* at the terminal time.

Theorem 1 (Reflection Principle, Theorem 2.21 in [23])**.** *For $a \in (0,\infty)$ and $t \in \mathbb{R}_+$,*

$$P(\{w \in \Omega \mid S_t \geq a\}) = P(\{w \in \Omega \mid |W(t,w)| \geq a\}) = \frac{2}{\sqrt{2\pi\delta^2 t}} \int_a^\infty e^{-\frac{x^2}{2\delta^2 t}} dx,$$

where $S_t = \max_{0\leq s\leq t} W(s,w)$. Similarly, for $b \in (-\infty, 0)$ and $t \in \mathbb{R}_+$,

$$P(\{w \in \Omega \mid \tilde{S}_t \leq b\}) = P(\{w \in \Omega \mid |W(t,w)| \geq -b\}) = \frac{2}{\sqrt{2\pi\delta^2 t}} \int_{-\infty}^b e^{-\frac{x^2}{2\delta^2 t}} dx,$$

where $\tilde{S}_t = \min_{0\leq s\leq t} W(s,w)$.

Definition 2. *A finite collection of m mutually independent Wiener processes $W_i(\cdot,\cdot) : [0,\infty) \times \Omega_i \to \mathbb{R}$, $i = 1,\ldots,m$, is called an m-dimensional Wiener process, where $W_i(\cdot,\cdot)$ is a Wiener process defined on the probability space $(\Omega_i,\mathcal{F}_i,P_i)$. For convenience, we denote the m Wiener processes $(W_1(\cdot,\cdot),\ldots,W_m(\cdot,\cdot))^\top$ by $\boldsymbol{W}(\cdot,\cdot)$, which maps from $[0,\infty)$ to $\mathbb{R}^m$, and its probability space by $(\boldsymbol{\Omega},\boldsymbol{\mathcal{F}},\boldsymbol{P})$.*

Therefore, for an m-dimensional Wiener process $\boldsymbol{W}(\cdot,\cdot)$, we have that for any $a_i > 0$, $i = 1,\ldots,m$, and $t \in \mathbb{R}_+$,

$$\begin{aligned}&\boldsymbol{P}(\{\boldsymbol{w} \in \boldsymbol{\Omega} \mid S_{1,t} \geq a_1,\ldots,S_{m,t} \geq a_m\})\\ &= \prod_{i=1}^m P_i(\{w_i \in \Omega_i \mid S_{i,t} \geq a_i\}),\end{aligned} \tag{3}$$

where $\boldsymbol{w} = (w_1,\ldots,w_m)^\top$ and $S_{i,t} = \max_{0\leq s\leq t} W_i(s,w_i)$.

B. Random Ordinary Differential Equations

In this subsection we formally present the concept of random ordinary differential equations (RODEs) that is of interest for this paper as we will solve their p-safety problem.

The type of RODE addressed in this paper is as follows:

$$\dot{\boldsymbol{x}}(s) = \boldsymbol{f}(\boldsymbol{x}(s), \boldsymbol{W}(s,\boldsymbol{w})), \tag{4}$$

where $\boldsymbol{x}(\cdot) : [0,\infty) \to \mathbb{R}^n$ and $\boldsymbol{W}(\cdot,\cdot) : [0,\infty) \times \boldsymbol{\Omega} \to \mathbb{R}^m$ is an m-dimensional Wiener process defined on the probability space $(\boldsymbol{\Omega},\boldsymbol{\mathcal{F}},\boldsymbol{P})$ equipped with the natural filtration.

We assume in what follows that the vector field $\boldsymbol{f} : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ satisfies the following two conditions:

1) $\boldsymbol{f}(\boldsymbol{x},\boldsymbol{d})$ is continuous over $\boldsymbol{x} \in \mathbb{R}^n$ and $\boldsymbol{d} \in \mathbb{R}^m$;
2) for each $\boldsymbol{d} \in \mathbb{R}^m$, $\boldsymbol{f}(\boldsymbol{x},\boldsymbol{d})$ is locally Lipschitz continuous over $\boldsymbol{x}$, i.e., for each $\boldsymbol{d} \in \mathbb{R}^m$ and each compact set $\tilde{X}$ in $\mathbb{R}^n$, there is some constant L such that
$$\|\boldsymbol{f}(\boldsymbol{x},\boldsymbol{d}) - \boldsymbol{f}(\boldsymbol{z},\boldsymbol{d})\| \leq L\|\boldsymbol{x} - \boldsymbol{z}\|, \forall \boldsymbol{x},\boldsymbol{z} \in \tilde{X},$$
where $\|\cdot\|$ denotes the usual Euclidean norm.

Consequently, according to [16], for the Wiener path $\boldsymbol{W}(\cdot,\boldsymbol{w}) : [0,\infty) \to \mathbb{R}^m$, there exists a unique continuously differentiable solution to (4) for some time interval. We denote the unique solution as $\boldsymbol{\phi}_{\boldsymbol{x}_0}^{\boldsymbol{W}_{\boldsymbol{w}}}(\cdot)$ with $\boldsymbol{\phi}_{\boldsymbol{x}_0}^{\boldsymbol{W}_{\boldsymbol{w}}}(0) = \boldsymbol{x}_0$.

Given a safe state set $X = \{\boldsymbol{x} \in \mathbb{R}^n \mid g(\boldsymbol{x}) \leq 0\}$ with $g(\cdot) : \mathbb{R}^n \to \mathbb{R}$ and a target set $\mathrm{TR} = \{\boldsymbol{x} \in \mathbb{R}^n \mid l(\boldsymbol{x}) \leq 0\}$ with $l(\cdot) : \mathbb{R}^n \to \mathbb{R}$, the *p*-safety problem for system (4) is defined as follows.

Definition 3. *Given a safe probability threshold $p \in (0,1)$, an initial state $\boldsymbol{x}_0$ is p-safe,*

1) *for a finite time horizon $[0,T]$ iff the probability that the induced trajectories of system* (4) *starting from $\boldsymbol{x}_0$ reach the target set* TR *at time instant $t = T$ while staying within the safe set X over the time horizon $[0,T]$ is larger than p, i.e.,*

$$\boldsymbol{P}\Big(\Big\{\boldsymbol{w} \in \boldsymbol{\Omega} \,\Big|\, \begin{array}{r}\forall s \in [0,T].\ \boldsymbol{\phi}_{\boldsymbol{x}_0}^{\boldsymbol{W}_{\boldsymbol{w}}}(s) \in X \bigwedge\\ \boldsymbol{\phi}_{\boldsymbol{x}_0}^{\boldsymbol{W}_{\boldsymbol{w}}}(T) \in \mathrm{TR}\end{array}\Big\}\Big) \geq p,$$

where $T \in [0,\infty)$.

2) for the infinite time horizon *iff the probability that the induced trajectories of system* (4) *starting from* $\boldsymbol{x}_0$ *stay within the safe set* X *over the infinite time horizon* $[0,\infty)$ *is larger than* p*, i.e.,*

$$\boldsymbol{P}(\{\boldsymbol{w}\in\boldsymbol{\Omega}\mid\forall s\in[0,\infty).\ \boldsymbol{\phi}^{\boldsymbol{W_w}}_{\boldsymbol{x}_0}(s)\in X\})\geq p.$$

The p*-safety problem is to identify a set of* p*-safe initial states* $\boldsymbol{x}_0$ *over both finite time horizons and the infinite time horizon.*

In this paper we will extend the existing qualitative reachability analysis methods for perturbed ODEs, i.e., ODEs with time-varying perturbation inputs, to solve the quantitative p-safety problem for RODEs.

III. Safety Verification

In this section we elucidate our method of addressing the p-safety problem for system (4) over both finite time horizons and the infinite time horizon by reducing stochastic reachability of RODEs to adversary reachability of ODEs. We first present our method for addressing the p-safety problem over finite time horizons in Subsection III-A and then extend this method, together with the robust invariant sets generation method for perturbed ODEs, to solve the p-safety problem over the infinite time horizon in Subsection III-B.

A. Safety Verification over Finite Time Horizons

This subsection focuses on solving the p-safety problem over finite time horizons. The solution consists of two steps. The first one is to identify a set of Wiener paths covering a probability mass of at least p. The second step is to construct a perturbed ODE based on the identified set of Wiener paths and compute an inner approximation of the robust backward reachable set over the specified time horizon $[0,T]$ for the constructed ODE. The robust backward reachable set over the time horizon $[0,T]$ is the set of initial states from which all trajectories of the ODE enter the target set TR at time $t=T$ while staying within the safe state set X throughout the time horizon $[0,T]$. By construction, this also constitutes a set of p-safe initial states for RODE (4), i.e., the construction computes an inner approximation of the exact set of p-safe initial states. This description is formally reflected in Theorem 2.

Theorem 2. *Suppose the probability of Wiener paths staying within a bounded set* $D\subset\mathbb{R}^m$ *over the time horizon* $[0,T]$ *is larger than* p*, i.e.,* $\boldsymbol{P}(\{\boldsymbol{w}\in\boldsymbol{\Omega}\mid\boldsymbol{W}(t,\boldsymbol{w})\in D,\forall t\in[0,T]\})\geq p$*, and* $\mathcal{D}$ *is the set of continuous functions mapping* $[0,T]$ *to* D*, i.e.,* $\mathcal{D}=\{\boldsymbol{d}(\cdot)\in\mathcal{C}^m[0,T]\mid\boldsymbol{d}(t)\in D,\forall t\in[0,T]\}$*. If* IN *is an inner approximation of the robust backward reachable set for perturbed* ODE (5) *over the time horizon* $[0,T]$*, with*

$$\dot{\boldsymbol{x}}(s)=\boldsymbol{f}(\boldsymbol{x}(s),\boldsymbol{d}(s)),s\in[0,T],\tag{5}$$

where $\boldsymbol{d}(\cdot)\in\mathcal{D}$ *is the perturbation input, then every state in the set* IN *is* p*-safe.*

Proof. Over the time horizon $[0,T]$, we denote the trajectory to ODE (5) with the perturbation input $\boldsymbol{d}(\cdot):[0,T]\to D$ and the initial state $\boldsymbol{x}_0$ by $\boldsymbol{\psi}^{\boldsymbol{d}}_{\boldsymbol{x}_0}(\cdot):[0,T]\to\mathbb{R}^n$. Therefore, the robust backward reachable set for perturbed ODE (5) is $\{\boldsymbol{x}_0\in\mathbb{R}^n\mid\forall t\in[0,T].\ \forall\boldsymbol{d}(\cdot)\in\mathcal{D}.\ \boldsymbol{\psi}^{\boldsymbol{d}}_{\boldsymbol{x}_0}(t)\in X\wedge\boldsymbol{\psi}^{\boldsymbol{d}}_{\boldsymbol{x}_0}(T)\in\text{TR}\}$, denoted by $\mathcal{R}^u$. Clearly, IN $\subseteq\mathcal{R}^u$.

Besides, we denote the set of Wiener paths staying within the bounded set $D\subset\mathbb{R}^m$ over the time horizon $[0,T]$ by $\mathcal{W}$. Obviously, $\mathcal{W}\subseteq\mathcal{D}$.

For $\boldsymbol{x}_0\in$ IN, we have that

$$\begin{aligned}&\boldsymbol{P}(\{\boldsymbol{w}\in\boldsymbol{\Omega}\mid\forall t\in[0,T].\ \boldsymbol{\phi}^{\boldsymbol{W_w}}_{\boldsymbol{x}_0}(t)\in X\wedge\boldsymbol{\phi}^{\boldsymbol{W_w}}_{\boldsymbol{x}_0}(T)\in\text{TR}\})\\&\geq A+B\geq A,\end{aligned}$$

where

$$A=\boldsymbol{P}\Big(\left\{\boldsymbol{w}\in\boldsymbol{\Omega}\;\middle|\;\begin{array}{l}\forall s\in[0,T].\ \boldsymbol{W}(\cdot,\boldsymbol{w})\in\mathcal{W}\bigwedge\\ \boldsymbol{\phi}^{\boldsymbol{W_w}}_{\boldsymbol{x}_0}(s)\in X\bigwedge\boldsymbol{\phi}^{\boldsymbol{W_w}}_{\boldsymbol{x}_0}(T)\in\text{TR}\end{array}\right\}\Big)$$

and

$$B=\boldsymbol{P}\Big(\left\{\boldsymbol{w}\in\boldsymbol{\Omega}\;\middle|\;\begin{array}{l}\forall s\in[0,T].\ \boldsymbol{W}(\cdot,\boldsymbol{w})\notin\mathcal{W}\bigwedge\\ \boldsymbol{\phi}^{\boldsymbol{W_w}}_{\boldsymbol{x}_0}(s)\in X\wedge\boldsymbol{\phi}^{\boldsymbol{W_w}}_{\boldsymbol{x}_0}(T)\in\text{TR}\end{array}\right\}\Big).$$

Moreover, since $\mathcal{W}\subseteq\mathcal{D}$, $\boldsymbol{W}(\cdot,\boldsymbol{w})\in\mathcal{D}$ if $\boldsymbol{W}(\cdot,\boldsymbol{w})\in\mathcal{W}$. Likewise, as $\boldsymbol{\phi}^{\boldsymbol{W_w}}_{\boldsymbol{x}_0}(s)=\boldsymbol{\psi}^{\boldsymbol{W_w}}_{\boldsymbol{x}_0}(s)$ for $s\in[0,T]$, it follows $\boldsymbol{\phi}^{\boldsymbol{W_w}}_{\boldsymbol{x}_0}(s)\in X$ for $s\in[0,T]$ and $\boldsymbol{\phi}^{\boldsymbol{W_w}}_{\boldsymbol{x}_0}(T)\in\text{TR}$ if $\boldsymbol{W}(\cdot,\boldsymbol{w})\in\mathcal{W}$. Thus,

$$\begin{aligned}&\boldsymbol{P}\Big(\left\{\boldsymbol{w}\in\boldsymbol{\Omega}\;\middle|\;\begin{array}{l}\forall s\in[0,T].\ \boldsymbol{W}(\cdot,\boldsymbol{w})\in\mathcal{W}\bigwedge\\ \boldsymbol{\phi}^{\boldsymbol{W_w}}_{\boldsymbol{x}_0}(s)\in X\wedge\boldsymbol{\phi}^{\boldsymbol{W_w}}_{\boldsymbol{x}_0}(T)\in\text{TR}\end{array}\right\}\Big)\\&=\boldsymbol{P}(\{\boldsymbol{w}\in\boldsymbol{\Omega}\mid\boldsymbol{W}(\cdot,\boldsymbol{w})\in\mathcal{W})\geq p.\end{aligned}$$

Hence, $\boldsymbol{P}(\{\boldsymbol{w}\in\boldsymbol{\Omega}\mid\forall s\in[0,T].\ \boldsymbol{\phi}^{\boldsymbol{W_w}}_{\boldsymbol{x}_0}(s)\in X\wedge\boldsymbol{\phi}^{\boldsymbol{w}}_{\boldsymbol{x}_0}(T)\in\text{TR}\})\geq p$. Definition 3 indicates that $\boldsymbol{x}_0$ is p-safe. □

Based on Theorem 2, a method for solving p-safety problems over finite time horizons is summarized in Alg. 1.

Algorithm 1 The Framework for Solving the p-Safety Problem over Finite Time Horizons via Reducing Stochastic Reachability to Adversary Reachability of ODEs

Require: RODE (4) and time horizon $[0,T]$; safe set X; target set TR; probability threshold $p\in(0,1)$ for safety.

Ensure: A set of p-safe initial states.

1) Obtain a set $\mathcal{W}$ of sample paths covering a probability mass of at least p via the reflection principle;
2) Construct a perturbed ODE (5) by regarding the sample paths in $\mathcal{W}$ as perturbation inputs;
3) Apply existing reachability techniques to the constructed ODE (5) for computing an inner approximation IN of the robust backward reachable set over the time horizon $[0,T]$;
4) Return the computed inner approximation IN of the set of p-safe initial states.

In practice, in order to facilitate computationally less expensive computations, the perturbed ODE (5) *in Alg. 1 can be further relaxed into another perturbed* ODE*, which is relatively easily manipulated with its trajectories including the ones of* ODE (5). We in the following use a simple example to illustrate the idea behind our method.

Example 1. *Consider a one-dimensional simple* RODE*,*

$$\dot{x}(s) = -x(s) + 10\sin\left(\frac{W(s,w)}{10}\right)x^3(s), s \in [0,T], \quad (6)$$

where $T = 1$*,* $X = \{x \in \mathbb{R} \mid g(x) \leq 0\}$ *with* $g(x) = x^2 - 0.9$*,* $\mathrm{TR} = \{x \in \mathbb{R} \mid l(x) \leq 0\}$ *with* $l(x) = x^2 - 0.5$*, and* $W(\cdot,\cdot) : [0,\infty) \times \Omega \to \mathbb{R}$ *is a standard Wiener process. The p-safety problem is to identify a set of* $(1 - 1.2 \times 10^{-6})$*-safe initial states.*

Step 1 of Alg. 1: Based on the reflection principle in Theorem 1 we identify the set $\mathcal{W} = \{W(\cdot,w) : [0,T] \to D \mid w \in \Omega\}$*, which is the set of all continuous Wiener paths staying within the interval* $D = (-5,5)$ *over the time horizon* $[0,T]$*, with probability of at least* $1 - 1.2 \times 10^{-6}$*, i.e.,*

$$P(\{w \in \Omega \mid W(\cdot,w) \in \mathcal{W}\}) \geq 1 - 1.2 \times 10^{-6}.$$

This is done as follows: Since

$$\begin{aligned} &P(\{w \in \Omega \mid W(t,w) \in (b,a), \forall t \in [0,1]\}) \\ &- P(\{w \in \Omega \mid \tau_a \wedge \tau_b \leq 1\}) \\ &+ P(\{w \in \Omega \mid \tau_a \leq 1\}) + P(\{w \in \Omega \mid \tau_b \leq 1\}) = 1 \end{aligned} \quad (7)$$

where $a > 0$ *and* $b < 0$*,* $\tau_a = \inf\{s \in [0,\infty) \mid W(s,w) \geq a\}$*,* $\tau_b = \inf\{s \in [0,\infty) \mid W(s,w) \leq b\}$ *and* $\tau_a \wedge \tau_b = \max\{\tau_b, \tau_a\}$*,*

$$\begin{aligned} &P(\{w \in \Omega \mid W(t,w) \in (b,a), \forall t \in [0,1]\}) \\ &\geq 1 - P(\{w \in \Omega \mid \tau_a \leq 1\}) - P(\{w \in \Omega \mid \tau_b \leq 1\}) \end{aligned}$$

holds. According to the reflection principle in Theorem 1, we have

$$\begin{aligned} &P(\{w \in \Omega \mid \tau_a \leq 1\}) \\ &= P(\{w \in \Omega \mid |W(1,w)| \geq a)\} = 2\frac{1}{\sqrt{2\pi}}\int_a^\infty e^{-\frac{x^2}{2}}dx \end{aligned}$$

and

$$\begin{aligned} &P(\{w \in \Omega \mid \tau_b \leq 1\}) \\ &= P(\{w \in \Omega \mid |W(1,w)| \geq -b)\} = 2\frac{1}{\sqrt{2\pi}}\int_{-\infty}^b e^{-\frac{x^2}{2}}dx. \end{aligned}$$

Therefore, we just need to solve the following optimization problem:

$$\begin{aligned} &\min\ a - b \\ &\text{s.t. } 1 - 2\frac{1}{\sqrt{2\pi}}\int_a^\infty e^{-\frac{x^2}{2}}dx \\ &\qquad - 2\frac{1}{\sqrt{2\pi}}\int_{-\infty}^b e^{-\frac{x^2}{2}}dx \geq 1 - 1.2 \times 10^{-6}, \\ &\quad a \geq 0, b \leq 0. \end{aligned} \quad (8)$$

The objective function $a - b$ *corresponds to the Lebesgue measure of the set* D*. Since* $1 - 2\frac{1}{\sqrt{2\pi}}\int_a^\infty e^{-\frac{x^2}{2}}dx - 2\frac{1}{\sqrt{2\pi}}\int_{-\infty}^b e^{-\frac{x^2}{2}}dx = 1 - 2\frac{1}{\sqrt{2\pi}}\int_a^\infty e^{-\frac{x^2}{2}}dx - 2\frac{1}{\sqrt{2\pi}}\int_{-b}^\infty e^{-\frac{x^2}{2}}dx$ *is monotonically increasing over* a *and monotonically decreasing over* b*, the simplest approach for solving the optimization* (8) *is linear search. Via solving* (8) *based on linear search, we obtain* $a = -b = 5.0$*.*

d_u	d_{s_1}	d_{s_2}	d_{s_3}	d_{s_4}	d_{s_5}	d_{s_6}	R
10	10	10	10	10	10	10	1

TABLE I

Parameters for solving the semi-definite program (11)*.* d_u *denotes the degree of the polynomial* $u(x,t)$*.* d_{s_i} *denotes the degree of the sum-of-squares polynomial* s_i*,* $i = 1,\ldots,6$*.*

Step 2 of Alg. 1: By regarding the Wiener paths $W(\cdot,w)$ *in* $\mathcal{W}$ *as perturbation inputs, we consider the perturbed* ODE*:*

$$\dot{x}(s) = -x(s) + 10\sin\left(\frac{d(s)}{10}\right)x^3(s), s \in [0,T], \quad (9)$$

where $T = 1$*,* $X = \{x \in \mathbb{R} \mid g(x) \leq 0\}$*,* $\mathrm{TR} = \{x \in \mathbb{R} \mid l(x) \leq 0\}$*,* $d(\cdot) : [0,1] \to (-5,5)$ *is the continuous perturbation input. Since* $\sin\frac{d}{10}$ *is monotonically increasing over* $d \in (-5,5)$*, we further relax* (9) *to* (10)

$$\dot{x}(s) = -x(s) + 10d(s)x^3(s), s \in [0,T], \quad (10)$$

where $T = 1$*,* $X = \{x \in \mathbb{R} \mid g(x) \leq 0\}$*,* $\mathrm{TR} = \{x \in \mathbb{R} \mid l(x) \leq 0\}$*,* $d(\cdot) : [0,1] \to [-\sin\frac{5}{10}, \sin\frac{5}{10}]$ *is the continuous perturbation input and* $D = \{d \in \mathbb{R} \mid h(d) \geq 0\}$ *with* $h(d) = \sin^2\frac{5}{10} - d^2$*. Clearly, the trajectories of Eq.* (10) *include the ones of Eq.* (9)*.*

Step 3 of Alg. 1: From [43] an inner approximation of the robust backward reachable set $\mathrm{IN} = \{x \mid u(x,0) \leq 0\}$ *for* ODE (10) *can be computed by solving the semi-definite program* (11)*:*

$$\begin{aligned} &\inf \boldsymbol{c}^\top \cdot \boldsymbol{m} \\ &\text{s. t.} \\ &-\mathcal{L}u(x,t) - s_1 g_R(x) - s_2 t(T-t) - s_3 h(d) \in \sum[x,t,d], \\ &u(x,t) - g(x) - s_4 g_R(x) - s_5 t(T-t) \in \sum[x,t], \\ &u(x,T) - l(x) - s_6 g_R(x) \in \sum[x], \end{aligned} \quad (11)$$

where $\boldsymbol{c}^\top \cdot \boldsymbol{m} = \int_{B_R} u(x,0)dx$*,* $\boldsymbol{m}$ *is the vector of moments of the Lebesgue measure over* B_R *indexed in the same basis in which the polynomial* $u(x,0)$ *with coefficients* $\mathbf{c}$ *is expressed, and* $\mathcal{L}u(x,t) = \partial_t u(x,t) + \nabla_x u(x,t) \cdot (-x + 10dx^3)$*.* $B_R = \{x \in \mathbb{R} \mid g_R(x) \geq 0\}$*, where* $g_R(x) = R - x^2$ *with* R *being a positive number such that* $X \subseteq B_R$ *and* $\partial X \cap \partial B_R = \emptyset$*.* $\sum[\cdot]$ *denotes the set of sum-of-squares polynomials over the argument. The minimum is over polynomial* $u(x,t)$ *and sum-of-squares polynomials* $s_1(x,t,d)$*,* $s_2(x,t,d)$*,* $s_3(x,t,d)$*,* $s_4(x,t)$*,* $s_5(x,t)$ *and* $s_6(x)$*.*

Step 4 of Alg. 1: We obtain an inner approximation $\mathrm{IN} = \{x \in B_R \mid u(x,0) \leq 0\}$*, which is illustrated in Fig. 1. The computation time is 45.68 seconds on an i7-7500U 2.70GHz CPU with 32G* RAM *running Windows 10. According to Theorem 2, every initial state in* IN *for* RODE (6) *is* $(1 - 1.2 \times 10^{-6})$*-safe. The parameters for solving* (11) *are presented in Table I.*

In Example 1, the semi-definite programming based method (11) is only applicable to perturbed polynomial ODEs with semi-algebraic safe state sets, semi-algebraic target sets and semi-algebraic perturbation sets, i.e., $\boldsymbol{f}(\boldsymbol{x},\boldsymbol{d}) \in \mathbb{R}[\boldsymbol{x},\boldsymbol{d}]$, $g(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$, $l(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$ and $h(\boldsymbol{d}) \in \mathbb{R}[\boldsymbol{d}]$. Actually, any existing (inner-approximate) reachability techniques for

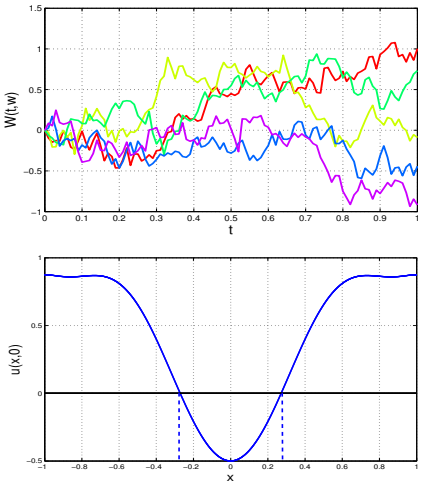

Fig. 1. An illustration of the computed p-safe initial states for Example 1. Above: Five sample paths of the Wiener process over the time horizon $[0, T]$ are presented. Below: The solid blue curve denotes $u(x, 0)$ computed by solving (11). The computed p-safe initial states are the states between the two dashed blue lines, i.e., IN $= \{x \in X \mid u(x, 0) \leq 0\}$.

perturbed ODEs can be used to implement Alg. 1. This is why we did not customize Alg. 1, thus providing more flexibility to users such that they can customize the algorithm themselves for the system of interest. For instance, if the perturbed ODE is not polynomial, we can use a reach-set computation method based on the time-dependent Hamilton-Jacobi equation [43] to compute an inner approximation of the robust backward reachable set. Besides, in Example 1 the set $\mathcal{W}$ of Wiener paths staying within a bounded set and having probability of at least p is not unique. However, the set $\mathcal{W}$ of the smallest Lebesgue measure is unique, which is used in Example 1 and can be easily concluded from the symmetric "bell curve" shape of the graph of a Gaussian. A set of perturbation inputs with the smallest Lebesgue measure is commonly preferred in practice since it generally results in less conservative results.

B. Safety Verification over the Infinite Time Horizon

This subsection focuses on solving the p-safety problem over the infinite time horizon.

Generally, it is more challenging to solve the p-safety problem over the infinite time horizon. Unlike safety problem over finite time horizons, since the probability for Wiener paths to stay within a bounded set always is zero, we generally cannot obtain a set of p-safe initial states for the infinite time horizon based on a set of bounded Wiener paths with a probability of at least $p \in (0, 1)$. Consequently, we propose a novel computational procedure of reducing the p-safety problem for the infinite time horizon to the one for finite time horizons, which consists of three steps. Based on the set of Wiener paths with probability one, the first step is to construct a perturbed ODE and compute a robust invariant set for the constructed ODE. This is the key step in our approach of solving the p-safety problem over the infinite time horizon, and this also limits our approach to system (4) with $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{W}(s, \boldsymbol{w}))$ satisfying

$$\exists B \in [0, \infty). \forall \boldsymbol{x} \in X. \forall s \in [0, \infty). \\ \forall \boldsymbol{w} \in \boldsymbol{\Omega}. \|\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{W}(s, \boldsymbol{w}))\| \leq B.$$

The robust invariant set is a set of initial states such that every possible trajectory to the ODE starting from them always stays within the set X. Also, the computed robust invariant set is also a set of p-safe initial states. Then we identify a finite time horizon, and a set of Wiener paths staying within a bounded set over the identified finite time horizon having a probability of at least p. Finally, we take the computed robust invariant set as the target set TR and apply the method in Subsection III-A to compute an inner approximation of the robust backward reachable set, therefore expanding the set of p-safe initial states. Every state $\boldsymbol{x}_0$ in the union of the computed robust invariant set and the computed inner approximation is p-safe over the infinite time horizon. The rationale behind these procedures is formally reflected in Theorem 3.

Theorem 3. *Suppose the probability of Wiener paths staying within a bounded set $D \subset \mathbb{R}^m$ over the time horizon $[0, \tau]$ is larger than p, i.e., $\boldsymbol{P}(\{\boldsymbol{w} \in \boldsymbol{\Omega} \mid \forall s \in [0, \tau]. \boldsymbol{W}(s, \boldsymbol{w}) \in D\}) \geq p$, $\mathcal{D}$ is the set of continuous functions mapping $[0, \tau]$ to D, i.e., $\mathcal{D} = \{\boldsymbol{d}(\cdot) \in \mathcal{C}^m[0, \tau] \mid \boldsymbol{d}(\cdot) : [0, \tau] \to D\}$. If* IN *is a set of initial states from which all trajectories to* ODE (12) *enter the target set* $\widetilde{\text{TR}}$ *at time $t = \tau$ while staying within the safe state set X over the time horizon $[0, \tau]$, where* $\widetilde{\text{TR}}$ *is a robust invariant set for* ODE (13) *such that all trajectories starting from it stay within the safe state set X forever, where*

$$\dot{\boldsymbol{x}}(s) = \boldsymbol{f}(\boldsymbol{x}(s), \boldsymbol{d}(s)), \tag{12}$$

with $\boldsymbol{d}(\cdot) \in \mathcal{D}$ being the perturbation input, and

$$\dot{\boldsymbol{x}}(s) = \boldsymbol{f}(\boldsymbol{x}(s), \boldsymbol{d}'(s)), \tag{13}$$

with $\boldsymbol{d}'(\cdot) \in \mathcal{C}^m[0, \infty)$ being the perturbation input. Then every initial state in IN$\cup\widetilde{\text{TR}}$ *is p-safe over the infinite time horizon.*

Proof. We denote the trajectory to ODE (12) with the perturbation input $\boldsymbol{d}(\cdot) : [0, \tau] \to D$ and the initial state $\boldsymbol{x}_0$ by $\boldsymbol{\psi}^{\boldsymbol{d}}_{\boldsymbol{x}_0}(\cdot) : [0, \tau] \to \mathbb{R}^n$. Also, we denote the set of Wiener paths staying within the bounded set $D \subset \mathbb{R}^m$ over the time horizon $[0, \tau]$ by $\mathcal{W}$. Clearly, $\mathcal{W} \subseteq \mathcal{D}$. We denote the trajectory to ODE (13) with the perturbation input $\boldsymbol{d}'(\cdot) : [0, \infty) \to \mathbb{R}^m$ and the initial state $\boldsymbol{x}_0$ by $\boldsymbol{\varphi}^{\boldsymbol{d}'}_{\boldsymbol{x}_0}(\cdot)$.

Since $\boldsymbol{\phi}^{\boldsymbol{W}_w}_{\boldsymbol{x}_0}(s) = \boldsymbol{\varphi}^{\boldsymbol{W}_w}_{\boldsymbol{x}_0}(s)$ for $\boldsymbol{W}(\cdot, \boldsymbol{w}) \in \mathcal{C}^m[0, \infty)$ and $t \in [0, \infty)$, we have that if $\boldsymbol{x}_0 \in \widetilde{\text{TR}}$,

$$\boldsymbol{P}(\{\boldsymbol{w} \in \boldsymbol{\Omega} \mid \forall s \in [0, \infty). \boldsymbol{\phi}^{\boldsymbol{W}_w}_{\boldsymbol{x}_0}(s) \in X\}) \\ = \boldsymbol{P}(\{\boldsymbol{w} \in \boldsymbol{\Omega} \mid \boldsymbol{W}(\cdot, \boldsymbol{w}) \in \mathcal{C}^m[0, \infty)\}) = 1 \geq p.$$

If $\boldsymbol{x}_0 \in$ IN, we have that

$$\boldsymbol{P}(\{\boldsymbol{w} \in \boldsymbol{\Omega} \mid \forall s \in [0, \infty). \boldsymbol{\phi}^{\boldsymbol{W}_w}_{\boldsymbol{x}_0}(s) \in X\}) \\ \geq \boldsymbol{P}(\{\boldsymbol{w} \in \boldsymbol{\Omega} \mid \forall s \in [0, \tau]. \boldsymbol{\phi}^{\boldsymbol{W}_w}_{\boldsymbol{x}_0}(s) \in X \wedge \boldsymbol{\phi}^{\boldsymbol{W}_w}_{\boldsymbol{x}_0}(\tau) \in \widetilde{\text{TR}}\}) \\ = A + B \geq A,$$

where

$$A = \boldsymbol{P}\Big(\Big\{\boldsymbol{w} \in \boldsymbol{\Omega} \;\Big|\; \begin{array}{l} \forall s \in [0, \tau]. \boldsymbol{W}(\cdot, \boldsymbol{w}) \in \mathcal{D} \bigwedge \\ \boldsymbol{\phi}^{\boldsymbol{W}_w}_{\boldsymbol{x}_0}(s) \in X \wedge \boldsymbol{\phi}^{\boldsymbol{W}_w}_{\boldsymbol{x}_0}(\tau) \in \widetilde{\text{TR}} \end{array}\Big\}\Big)$$

and

$$B = \boldsymbol{P}\Big(\left\{ \boldsymbol{w} \in \boldsymbol{\Omega} \;\middle|\; \begin{array}{l} \forall s \in [0,\tau].\ \boldsymbol{W}(\cdot,\boldsymbol{w}) \notin \mathcal{D} \bigwedge \\ \boldsymbol{\phi}_{\boldsymbol{x}_0}^{\boldsymbol{W}_{\boldsymbol{w}}}(s) \in X \bigwedge \boldsymbol{\phi}_{\boldsymbol{x}_0}^{\boldsymbol{W}_{\boldsymbol{w}}}(\tau) \in \widetilde{\mathrm{TR}} \end{array} \right\} \Big).$$

Since $\mathcal{W} \subseteq \mathcal{D}$, $\boldsymbol{W}(\cdot,\boldsymbol{w}) \in \mathcal{D}$ if $\boldsymbol{W}(\cdot,\boldsymbol{w}) \in \mathcal{W}$. Also, since $\boldsymbol{\phi}_{\boldsymbol{x}_0}^{\boldsymbol{W}_{\boldsymbol{w}}}(s) = \boldsymbol{\psi}_{\boldsymbol{x}_0}^{\boldsymbol{W}_{\boldsymbol{w}}}(s)$ for $s \in [0,\tau]$,

$$\begin{aligned} &\boldsymbol{P}\Big(\left\{ \boldsymbol{w} \in \boldsymbol{\Omega} \;\middle|\; \begin{array}{l} \forall s \in [0,\tau].\ \boldsymbol{W}(\cdot,\boldsymbol{w}) \in \mathcal{D} \bigwedge \\ \boldsymbol{\phi}_{\boldsymbol{x}_0}^{\boldsymbol{W}_{\boldsymbol{w}}}(s) \in X \wedge \boldsymbol{\phi}_{\boldsymbol{x}_0}^{\boldsymbol{W}_{\boldsymbol{w}}}(\tau) \in \widetilde{\mathrm{TR}} \end{array} \right\} \Big) \\ &= \boldsymbol{P}(\{\boldsymbol{w} \in \boldsymbol{\Omega} \mid \boldsymbol{W}(\cdot,\boldsymbol{w}) \in \mathcal{D}\}) \geq p. \end{aligned} \tag{14}$$

Consequently, $\boldsymbol{P}(\{\boldsymbol{w} \in \boldsymbol{\Omega} \mid \forall s \in [0,\infty).\ \boldsymbol{\phi}_{\boldsymbol{x}_0}^{\boldsymbol{W}_{\boldsymbol{w}}}(s) \in X\}) \geq p$. Definition 3 indicates that $\boldsymbol{x}_0 \in \mathrm{IN} \cup \widetilde{\mathrm{TR}}$ is p-safe. □

Reflecting the constructions from the proof of Theorem 3, our method for solving p-safety problem over the infinite time horizon is summarized in Alg. 2.

Algorithm 2 The Framework for Solving the p-Safety Problem over the Infinite Time Horizon via Reducing Stochastic Reachability to Adversary Reachability of ODEs

Require: RODE (4); safe state set X; probability threshold $p \in (0,1)$ for safety.

Ensure: A set of p-safe initial states.

1) Obtain a perturbed ODE (13) by regarding the set of all sample paths as perturbation inputs;
2) Apply robust invariant sets generation techniques to the obtained ODE for computing a robust invariant set $\widetilde{\mathrm{TR}}$;
3) Choose a finite time horizon $[0,\tau]$;
4) Obtain an inner approximation IN by applying Alg. 1 to RODE (4) with the safe set X, target set $\widetilde{\mathrm{TR}}$, time horizon $[0,\tau]$ and safety level p;
5) Return the set $\mathrm{IN} \cup \widetilde{\mathrm{TR}}$, which constitutes a (in general not maximal) set of p-safe initial states.

Like in Subsection III-A, in order to facilitate computations the perturbed ODEs (12) and (13) in Alg. 2 can be further relaxed into another perturbed ODEs, which are relatively easily manipulated with their trajectories including the ones of ODEs (12) and (13) respectively. Similarly, we use a simple example to illustrate the idea behind our method as well.

Example 2. *Consider a one-dimensional simple* RODE *again,*

$$\dot{x}(s) = -x(s) + 0.09x^2(s) + 0.5\sin(\frac{W(s,w)}{10})x^3(s) \tag{15}$$

with $X = \{x \in \mathbb{R} \mid g(x) \leq 0\}$ *with* $g(x) = x^2 - 2$, *and the stochastic process* $W(s,w) : [0,\infty) \times \Omega \to \mathbb{R}$ *is a standard Wiener process. The p-safety problem considered for this example is to identify a set of* 1*-safe initial states.*

Step 1 of Alg. 2: since $\sin(\cdot) : \mathbb{R} \to [-1,1]$, *by regarding* $\sin(\frac{W(\cdot,\cdot)}{10}) : [0,\infty) \times \Omega \to [-1,1]$ *as perturbation inputs* $d(\cdot) : [0,\infty) \to [-1,1]$, *we consider the perturbed* ODE

$$\dot{x}(s) = -x(s) + 0.09x^2(s) + 0.5d(s)x^3(s) \tag{16}$$

d_u	d_{s_1}	d_{s_2}	d_{s_3}	g_R
8	8	8	8	$2.1 - x^2$

TABLE II
Parameters for solving the semi-definite program (17) *for Example 2.* d_u *denotes the degree of the polynomial* $u(x)$. d_{s_i} *denotes the degree of the sum-of-squares polynomial* s_i, $i = 1,\ldots,3$.

d_u	d_{s_1}	d_{s_2}	d_{s_3}	d_{s_4}	d_{s_5}	d_{s_6}	R
8	8	8	8	8	8	8	2.1

TABLE III
Parameters for solving the program (11) *for Example 2.*

where $X = \{x \in \mathbb{R} \mid g(x) \leq 0\}$ *and* $d(\cdot) : [0,\infty) \to D$ *is the perturbation with* $D = \{d \in \mathbb{R} \mid h(d) \geq 0\}$ *and* $h(d) = 1 - d^2$. *Clearly, the trajectories of* (16) *include the ones of* (15).

Step 2 of Alg. 2: We compute a robust invariant set of perturbed ODE (16) *such that every trajectory starting from it will always stay within the safe set* X, *regardless of perturbation inputs* $d(\cdot) : [0,\infty) \to [-1,1]$. *From [45], a robust invariant set* $\mathcal{R} = \{x \in X \mid u(x) \leq 0\}$ *of perturbed* ODE (16) *could be computed by solving the semi-definite program* (17)*:*

$$\begin{aligned} &\inf \boldsymbol{c}^\top \cdot \boldsymbol{m} \\ &\text{s. t.} \\ &-\mathcal{L}u(x) - s_1 h(d) - s_2 g_R(x) \in \sum[x,d], \\ &(1+g^2(x))u(x) - g(x) - s_3 g_R(x) \in \sum[x], \end{aligned} \tag{17}$$

where $\boldsymbol{c}^\top \cdot \boldsymbol{m} = \int_{B_R} u(x)dx$ *is the vector composed of unknown coefficients in* $u(x) \in \mathbb{R}[x]$, $\boldsymbol{m}$ *is the constant vector computed by integrating the monomials in* $u(x)$ *over* B_R, $B_R = \{x \in \mathbb{R} \mid g_R(x) \geq 0\}$ *with* $g_R(x) \in \mathbb{R}[x]$ *such that* $X \subseteq B_R$ *and* $\partial X \cap \partial B_R = \emptyset$, *and* $\mathcal{L}u(x) = \nabla_x u(x) \cdot (-x + 0.09x^2 + 0.5dx^3)$. $\sum[\cdot]$ *denotes the set of sum-of-squares polynomials over the argument. The minimum is over the polynomial* $u(x)$ *and sum-of-squares polynomials* $s_1(x,d)$, $s_2(x,d)$, *and* $s_3(x)$.

The computed robust invariant set $\widetilde{\mathrm{TR}} = \{x \in B_R \mid u(x) \leq 0\}$ *for* ODE (16) *is illustrated in Fig. 2. Obviously, it is a set of* 1*-safe initial states for* RODE (15). *The parameters in solving* (17) *are presented in Table II. The computation time is 4.70 seconds.*

Step 3 of Alg. 2: We choose the time horizon $[0,\tau]$ *with* $\tau = 1$.

Step 4 of Alg. 2: Via taking the computed robust invariant set $\widetilde{\mathrm{TR}} = \{x \in B_R \mid u(x) \leq 0\}$ *as the target set, we further compute a set* IN *of p-safe initial states such that*

$$P(\{w \in \Omega \mid \forall s \in [0,\tau].\ \phi_{\boldsymbol{x}_0}^{W_w}(s) \in X \wedge \phi_{\boldsymbol{x}_0}^{W_w}(\tau) \in \widetilde{\mathrm{TR}}\}) \geq p,$$

where $\tau = 1$. *Like Example 1, we first identify a set* $\mathcal{W}$ *of Wiener paths. Since* $p = 1$, *therefore, we use all of Wiener paths. That is,* $\mathcal{W} = \{W(\cdot,w) \in \mathcal{C}^1[0,\tau] \mid w \in \Omega\}$. *The probability* $P(\{w \in \Omega \mid W(\cdot,w) \in \mathcal{W}\})$ *is equal to* 1. *An inner-approximation* $\mathrm{IN} = \{x \in B_R \mid u'(x,0) \leq 0\}$, *which is also illustrated in Fig. 2, of the robust backward reachable set for* ODE (16) *with* $d(\cdot) : [0,1] \to D$ *is obtained by solving* (11). *The parameters in solving* (11) *are presented in Table III. The computation time is* 31.35 *seconds.*

Step 5 of Alg. 2: We obtain a set $\mathrm{IN} \cup \widetilde{\mathrm{TR}}$. *According to Theorem 3, every state in* $\mathrm{IN} \cup \widetilde{\mathrm{TR}}$ *is* 1*-safe for* RODE (15).

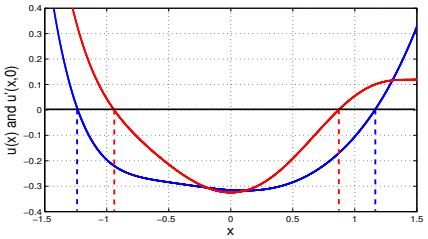

Fig. 2. An illustration of 1-safe initial states for Example 2. Red and blue solid curves denote $u(x)$ and $u'(x,0)$, respectively. The computed robust invariant set $\widetilde{\mathrm{TR}}$ is the set of states between the two dashed red lines. The computed inner approximation IN of the robust backward reachable set over the time horizon $[0,\tau]$ is the set of states between the two dashed blue lines.

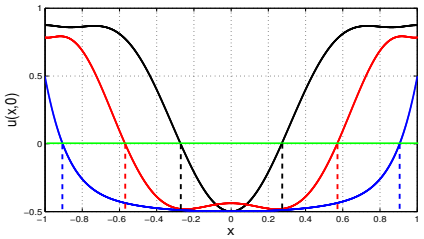

Fig. 3. An illustration of sets of p-safe initial states for Example 3. The states between the two dashed black lines, red lines and blue lines, are $(1-1.2\times 10^{-6})$-safe, 0.90-safe and 0.36-safe, respectively.

Like Example 1, if the perturbed ODE is not polynomial, we can use other reach-set computation methods such as the time-independent Hamilton-Jacobi equation based method in [45] to compute an approximation of the maximal robust invariant set. Besides, a finite time horizon $[0,\tau]$ is required for computations to further expand the set of p-safe initial states in Alg. 2. Generally, a bigger τ corresponds to a bounded set D with larger Lebesgue measure (the set D is defined in Theorem 3, which is a bounded set such that the probability of Wiener paths staying within it over the time horizon $[0,\tau]$ is larger than p.), which may result in more conservative sets. We would consider the choice of appropriate τ in future work.

IV. Experiments

In this section we illustrate our approach on five examples based on solving the programs (11) and (17), where three examples are on safety verification over finite time horizons and two examples on safety verification over the infinite time horizon. All computations were performed on an i7-7500U 2.70 GHz CPU with 32 GB RAM running Windows 10.

A. Safety Verification over Finite Time Horizons

In this subsection we illustrate our approach for safety verification over finite time horizons on three examples.

Example 3. *Consider the* RODE (6) *described in Example 1 again. In this example we discuss the effect of the probability threshold $p\in(0,1)$ on the computed set of p-safe initial states over finite time horizons.*

We first use the set $\mathcal{W}$ of all Wiener paths $W(\cdot,w):[0,T]\to(-\infty,\infty)$ to attempt computing a set of 1*-safe initial states. That is, $\mathcal{W}=\{W(\cdot,w):[0,T]\to(-\infty,\infty)\mid w\in\Omega\}$ and $P(\{w\in\Omega\mid W(\cdot,w)\in\mathcal{W}\})=1$. Thus, the set D in* (16) *is equal to $\{d\in\mathbb{R}\mid h(d)\geq 0\}$ with $h(d)=1-d^2$. Via solving the semi-definite program* (11) *with the parameters listed in Table I, we obtain an empty set of* 1*-safe initial states, which is a correct but useless inner approximation.*

Then we use the set $\mathcal{W}$ of Wiener paths $W(\cdot,w):[0,T]\to(-2,2)$. That is, $\mathcal{W}=\{W(\cdot,w):[0,T]\to(-2,2)\mid w\in\Omega\}$. Its probability is larger than 0.90*, i.e., $P(\{w\in\Omega\mid W(\cdot,w):[0,T]\to(-2,2)\})\geq 0.90$. Thus, the set D in* (10) *is equal to $\{d\in\mathbb{R}\mid h(d)\geq 0\}$ with $h(d)=\sin^2\frac{2}{10}-d^2$. Via solving the semi-definite program* (11) *with the parameters listed in Table I, we obtain a set of* 0.90*-safe initial states, which is also illustrated in Fig. 3. The computational time is* 48.24 *seconds.*

Finally, we use the set $\mathcal{W}$ of Wiener paths $W(\cdot,w):[0,T]\to(-1,1)$. Its probability is larger than 0.36*, i.e., $P(\{w\in\Omega\mid W(\cdot,w):[0,T]\to(-1,1)\})\geq 0.36$. Thus, the set D in* (16) *is equal to $\{d\in\mathbb{R}\mid h(d)\geq 0\}$ with $h(d)=\sin^2\frac{1}{10}-d^2$. Via solving the semi-definite program* (11) *with the parameters listed in Table I, we obtain a set of* 0.36*-safe initial states, which is illustrated in Fig. 3. The computation time here is* 51.32 *seconds.*

By choosing different probability levels p, we can separate the state space into several safe levels. For instance, we can observe from Fig. 3 that the computed set of p-safe initial states expands with p decreasing. However, the safe level is decreasing.

Example 4. *Consider a model for the horizontal slow drift motion of a moored floating platform or ship responding to incoming irregular waves from [25]:*

$$\ddot{x}(s)+a_0\dot{x}(s)+\beta^2x(s)=(T_0-\alpha_0\dot{x}(s))\eta W(s,w), \quad (18)$$

which is equivalent to the two-dimensional first-order RODE*:*

$$\begin{aligned}\dot{x}(s)&=y(s)\\ \dot{y}(s)&=-a_0y(s)-\beta^2x(s)+(T_0-\alpha_0y(s))\eta W(s,w),\end{aligned} \quad (19)$$

where $W(\cdot,\cdot)$ is 1*-dimensional standard Wiener process, $a_0=1$, $\beta=1$, $T_0=1$, $\alpha_0=1$, $\eta=0.01$, $T=1$, $X=\{\boldsymbol{x}\mid g(\boldsymbol{x})\leq 0\}$ with $g(\boldsymbol{x})=x^2+y^2-2$ and* TR $=\{\boldsymbol{x}\mid l(\boldsymbol{x})\leq 0\}$ *with $l(\boldsymbol{x})=(x-0.2)^2+(y-0.2)^2-0.25$.*

Since $W(\cdot,\cdot)$ is a 1*-dimensional standard Wiener process and is unbounded, it is impossible to compute a non-trivial set of* 1*-safe initial states. The considered p-safety problem is to identify a set of* 0.9*-safe initial states over the time $[0,T]$.*

We identify the set $\mathcal{W}$ of Wiener paths $W(\cdot,w):[0,T]\to(-2,2)$, i.e., $\mathcal{W}=\{W(\cdot,w):[0,T]\to(-2,2)\mid w\in\Omega\}$. Its probability is at least 0.90*, i.e., $P(\{w\in\Omega\mid W(\cdot,w):[0,T]\to(-2,2)\})\geq 0.9$. Thus, the set D in this example equals $\{d\in\mathbb{R}\mid h(d)\geq 0\}$ with $h(d)=4-d^2$. Via solving the semi-definite program* (11) *with the parameters in Table IV, we obtain a set of* 0.9*-safe initial states, which is illustrated in Fig. 4. The computation time amounts to 94.25 seconds.*

In order to shed light on the effect of stochastic perturbations on the system, we further consider the system free of stochastic perturbations. When the stochastic perturbations are not taken into account, i.e., $W(s,w)\equiv 0$ for $s\in[0,T]$ in

d_u	d_{s_1}	d_{s_2}	d_{s_3}	d_{s_4}	d_{s_5}	d_{s_6}	R
10	10	10	10	10	10	10	2.1

TABLE IV
Parameters for solving (11) *for Example 4.*

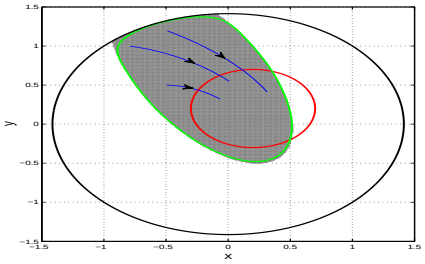

Fig. 4. An illustration of 0.9-safe initial states for Example 4. The black and red curves denote the boundary of the safe set X and the target set TR, respectively. The green curve denotes the boundary of the computed set of 0.9-safe initial states over the time horizon $[0, T]$. The gray region denotes the reach-avoid set corresponding to Eq. (19) with $W(s, w) \equiv 0$. Blue curves denote trajectories of RODE (19) over the time horizon $[0, T]$.

(19), *the reach-avoid set, which is a set of initial states such that the system* (19) *enters the target set* TR *at* $t = T$ *while staying inside the set* X *before the target hitting time, is shown in Fig. 4. It is estimated by simulation techniques. From Fig. 4 we observed that the computed set of* 0.9*-safe initial states is close to the reach-avoid set.*

Example 5. *The dynamics of a car in the two dimensions* $(x_1, x_2)^\top$ *of the plane are governed by Newton's law:*

$$\boldsymbol{f}(t) = m\boldsymbol{a}(t),$$

where $\boldsymbol{a}(t)$ *is the acceleration (in vectorial form),* m *is the mass of the car, and* $\boldsymbol{f}(t)$ *is a vector of (unknown) forces acting on the car. Let us model* $\frac{\boldsymbol{f}(t)}{m}$ *as a two-dimensional Wiener process [34]:*

$$\frac{d^2x_1}{dt^2} = W_1(t, w_1), \frac{d^2x_2}{dt^2} = W_2(t, w_2),$$

which can be written as a first-order RODE*:*

$$\begin{aligned} \frac{dx_1}{dt} &= x_3(t), \frac{dx_2}{dt} = x_4(t), \\ \frac{dx_3}{dt} &= W_1(t, w_1), \frac{dx_4}{dt} = W_2(t, w_2), \end{aligned}$$

where $T = 1$, $X = \{\boldsymbol{x} \in \mathbb{R}^4 \mid g(\boldsymbol{x}) \leq 0\}$ *with* $g(\boldsymbol{x}) = \sum_{i=1}^{2} x_i^2 + \sum_{i=3}^{4}(x_i - 0.5)^2 - 1$, TR $= \{\boldsymbol{x} \in \mathbb{R}^4 \mid l(\boldsymbol{x}) \leq 0\}$ *with* $l(\boldsymbol{x}) = \sum_{i=1}^{2}(x_i - 0.5)^2 + \sum_{i=3}^{4}(x_i - 0.5)^2 - 0.25$.

When setting $x_3 := x_3 - 0.5$ *and* $x_4 := x_4 - 0.5$*, we obtain the* RODE*:*

$$\begin{aligned} \frac{dx_1}{dt} &= x_3(t) + 0.5, \frac{dx_2}{dt} = x_4(t) + 0.5, \\ \frac{dx_3}{dt} &= W_1(t, w_1), \frac{dx_4}{dt} = W_2(t, w_2). \end{aligned} \tag{20}$$

where $T = 1$, $X = \{\boldsymbol{x} \in \mathbb{R}^4 \mid g(\boldsymbol{x}) \leq 0\}$ *with* $g(\boldsymbol{x}) = \sum_{i=1}^{4} x_i^2 - 1$, TR $= \{\boldsymbol{x} \in \mathbb{R}^4 \mid l(\boldsymbol{x}) \leq 0\}$ *with* $l(\boldsymbol{x}) = \sum_{i=1}^{2}(x_i - 0.5)^2 + \sum_{i=3}^{4} x_i^2 - 0.25$.

In this model $\boldsymbol{W}(\cdot, \cdot) = (W_1(\cdot, \cdot), W_2(\cdot, \cdot))^\top$ *is a* $2-$*dimensional Wiener process with* $\delta = 0.005$*. This process is unbounded, therefore it is impossible to compute a non-trivial set of* 1*-safe initial states. The* p*-safety problem we consider is to identify a set of* 0.8*-safe initial states over time horizon* $[0, T]$*. We identify the set* $\mathcal{W}$ *of Wiener paths* $\boldsymbol{W}(\cdot, \boldsymbol{w}) : [0, T] \to (-0.01, 0.01) \times (-0.01, 0.01)$*, i.e.,* $\mathcal{W} = \{\boldsymbol{W}(\cdot, \boldsymbol{w}) : [0, T] \to (-0.01, 0.01) \times (-0.01, 0.01) \mid \boldsymbol{w} \in \boldsymbol{\Omega}\}$*, with probability mass of at least* 0.8*, i.e.,* $\boldsymbol{P}(\{\boldsymbol{w} \in \boldsymbol{\Omega} \mid \boldsymbol{W}(\cdot, \boldsymbol{w}) : [0, T] \to (-0.01, 0.01) \times (-0.01, 0.01)\}) \geq 0.8$*. Thus, the set* D *in this example is equal to* $\{\boldsymbol{d} \in \mathbb{R}^2 \mid h_1(\boldsymbol{d}) \geq 0, h_2(\boldsymbol{d}) \geq 0\}$ *with* $h_1(\boldsymbol{d}) = 0.01^2 - d_1^2$ *and* $h_2(\boldsymbol{d}) = 0.01^2 - d_2^2$*. Via solving the semi-definite program* (11) *with the parameters listed in Table V, we obtain a set of* 0.8*-safe initial states illustrated in Fig. 6. The computation time here amounts to 175.84 seconds.*

Like Example 4, we also estimate the reach-avoid set, which is obtained by simulation techniques when the stochastic perturbations are not taken into account, i.e., $W_1(s, w_1) \equiv 0$ *and* $W_2(s, w_2) \equiv 0$ *for* $s \in [0, T]$ *in* (19)*. The reach-avoid set is shown in Fig. 6.*

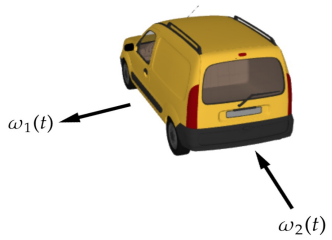

Fig. 5. An illustration of the car dynamic model.

d_u	d_{s_1}	d_{s_2}	d_{s_3}	d_{s_4}	d_{s_5}	d_{s_6}	R
6	6	6	6	6	6	6	1.1

TABLE V
Parameters for solving (11) *for Example 4.*

B. Safety Verification over the Infinite Time Horizon

In this subsection we illustrate our approach for the infinite time horizon verification on two examples.

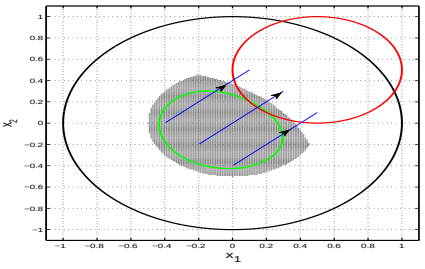

Fig. 6. An illustration of 0.8-safe initial states for Example 5 on the plane $x_1 - x_2$ with $x_3 = x_4 = 0$. The black curve denotes the boundary of the set X. The red curve denotes the boundary of the set TR. The green curve denotes the boundary of the computed set of 0.8-safe initial states over the time horizon $[0, T]$. The gray region denotes the reach-avoid set corresponding to Eq. (20) with $W_1(s, w_1) \equiv 0$ and $W_2(s, w_2) \equiv 0$. The blue curves denote trajectories of RODE (20) over time horizon $[0, T]$.

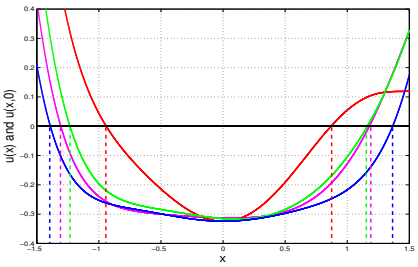

Fig. 7. An illustration of sets of p-safe initial states for Example 6. The states between the two dashed red curves are the 1-safe initial states falling within the computed robust invariant set. The states between the two dashed green curves are the 1-safe initial states falling within the computed backward reachable set with $T = 1$. The states between the two dashed purple curves are the 1-safe initial states falling within the computed backward reachable set with $T = 1.5$. The states between the two dashed blue curves are the $(1 - 1.2 \times 10^{-6})$-safe initial states falling within the computed robust backward reachable set with $T = 1$.

Example 6. *Consider the* RODE (15) *in Example 2 again. In this example we discuss the effect of the probability threshold* $p \in (0, 1)$ *and the time horizon* $[0, \tau]$ *on the computed set of* p*-safe initial states over the infinite time horizon.*

We use the robust invariant set $\widetilde{\text{TR}}$ *computed in Example 2. Then we first choose the time horizon* $[0, 1.5]$ *and the set* $\mathcal{W}$ *of Wiener paths in* $\mathcal{C}^1[0, \infty)$ *such that* $W(\cdot, w) : [0, 1.5] \to \mathbb{R}$*. That is,* $\mathcal{W} = \{W(\cdot, w) \in \mathcal{C}^1[0, 1.5] \mid w \in \Omega\}$ *includes the set of all continuous Wiener paths. Its probability measure is 1. Thus, the set* D *in* (16) *is* $\{d \in \mathbb{R} \mid h(d) \geq 0\}$ *with* $h(d) = 1 - d^2$*. The computed inner-approximation* IN *over the time horizon* $[0, 1.5]$ *is illustrated in Fig. 7. The computation time is* 31.47 *seconds.*

Besides we choose the time horizon $[0, 1]$ *again and the set* $\mathcal{W}$ *of Wiener paths in* $\mathcal{C}^1[0, \infty)$ *such that* $W(\cdot, w) : [0, 1] \to (-5, 5)$*. That is,* $\mathcal{W} = \{W(\cdot, w) \in \mathcal{C}^1[0, 1] \mid w \in \Omega\}$*. Its probability measure is larger than* $1 - 1.2 \times 10^{-6}$*. Thus, the set* D *in* (16) *is* $\{d \in \mathbb{R} \mid h(d) \geq 0\}$ *with* $h(d) = \sin^2 \frac{5}{10} - d^2$*. The computed inner approximation* IN *over the time horizon* $[0, 1]$ *is also illustrated in Fig. 7. The computation time here is* 31.80 *seconds.*

For ease of comparison, Fig. 7 also presents the set of 1*-safe initial states, which was computed in Example 2.*

From the results illustrated in Fig. 7, we observe that a less conservative set of p*-safe initial states could be computed using a larger time horizon for this example when the same set of Wiener paths is used. For instance, we can obtain a less conservative set of* 1*-safe initial states using the time horizon* $[0, 1.5]$ *rather than the time horizon* $[0, 1]$ *when the set of all continuous Wiener paths is used. However, one can further reduce this conservativeness by only considering a subset of Wiener paths rather than all the Wiener paths. For instance, a* $(1-1.2\times10^{-6})$*-safe initial state is practically* 1*-safe. However, the set of* $(1 - 1.2 \times 10^{-6})$*-safe initial states computed based on the set of continuous Wiener paths with a probability of at least* $(1 - 1.2 \times 10^{-6})$ *over the time horizon* $[0, 1]$ *is larger than the set of* 1*-safe initial states computed based on the set of all continuous Wiener paths over the time horizon* $[0, 1.5]$*.*

Example 7. *Consider a seven-dimensional academic example presented below,*

$$\begin{aligned}
\dot{x}_1 &= -(\sqrt{1.5}\sin(\frac{W_1(s, w_1)}{10}) + 2)x_1 + 0.5x_2\\
\dot{x}_2 &= -(\sqrt{1.5}\sin(\frac{W_2(s, w_2)}{10}) + 2)x_2 + 0.4x_3\\
\dot{x}_3 &= -x_3 + 0.5x_4\\
\dot{x}_4 &= -x_4 + 0.7x_5\\
\dot{x}_5 &= -x_5 + 0.6x_6\\
\dot{x}_6 &= -x_6 + 0.8x_7\\
\dot{x}_7 &= -x_7 + \sqrt{1.5}\sin(\frac{W_1(s, w_1)}{10})x_6 + 10x_1^2\\
&\qquad + x_2^2 - x_3^2 - x_4^2 + x_5^2
\end{aligned} \tag{21}$$

with $X = \{\boldsymbol{x} \in \mathbb{R}^7 \mid g(\boldsymbol{x}) \leq 0\}$*,* $g(\boldsymbol{x}) = \sum_{i=1}^7 x_i^2 - 0.25$ *and the stochastic process* $\boldsymbol{W}(\cdot, \cdot) = (W_1(\cdot, \cdot), W_2(\cdot, \cdot))^\top$ *being a 2-dimensional standard Wiener process. The* p*-safety problem for this example is to identify a set of* 0.98*-safe initial states.*

Like in Example 2, since $\sin(\cdot) : \mathbb{R} \to [-1, 1]$*, by regarding* $\sin(\frac{W_1(\cdot,\cdot)}{10}) : [0, \infty) \times \Omega_1 \to [-1, 1]$ *and* $\sin(\frac{W_2(\cdot,\cdot)}{10}) : [0, \infty) \times \Omega_2 \to [-1, 1]$ *as perturbation inputs* $d_1(\cdot) : [0, \infty) \to [-1, 1]$ *and* $d_2(\cdot) : [0, \infty) \to [-1, 1]$ *respectively, we consider the perturbed* ODE

$$\begin{aligned}
\dot{x}_1 &= -(\sqrt{1.5}d_1(s) + 2)x_1 + 0.5x_2\\
\dot{x}_2 &= -(\sqrt{1.5}d_2(s) + 2)x_2 + 0.4x_3\\
\dot{x}_3 &= -x_3 + 0.5x_4\\
\dot{x}_4 &= -x_4 + 0.7x_5\\
\dot{x}_5 &= -x_5 + 0.6x_6\\
\dot{x}_6 &= -x_6 + 0.8x_7\\
\dot{x}_7 &= -x_7 + \sqrt{1.5}d_1(s)x_6 + 10x_1^2\\
&\qquad + x_2^2 - x_3^2 - x_4^2 + x_5^2
\end{aligned} \tag{22}$$

where $X = \{\boldsymbol{x} \in \mathbb{R}^7 \mid g(\boldsymbol{x}) \leq 0\}$*,* $\boldsymbol{d}(\cdot) : [0, \infty) \to D$ *is the perturbation,* $D = \{\boldsymbol{d} \in \mathbb{R}^2 \mid h_1(\boldsymbol{d}) \geq 0, h_2(\boldsymbol{d}) \geq 0\}$ *with* $h_1(\boldsymbol{d}) = 1 - d_1^2$ *and* $h_2(\boldsymbol{d}) = 1 - d_2^2$*. Clearly, the trajectories of* (22) *include the ones of* (21)*.*

We first compute a robust invariant set of perturbed ODE (22) *such that every trajectory starting from it will always stay within the safe set* X*, regardless of perturbation inputs* $\boldsymbol{d}(\cdot) : [0, \infty) \to [-1, 1]^2$*. Via solving the semi-definite program* (17)*, we obtain a robust invariant set* $\widetilde{\text{TR}} = \{\boldsymbol{x} \in B_R \mid u(\boldsymbol{x}) \leq 0\}$ *for* ODE (22)*, which is illustrated in Fig. 8–10. Obviously, it is a set of* 1*-safe initial states for* RODE (21)*. The parameters in solving* (17) *are presented in Table VI and the computation time is 320.65 seconds.*

Then we choose the time horizon $[0, 2]$ *and identify the set* $\mathcal{W}$ *of Wiener paths* $\boldsymbol{W}(\cdot, \boldsymbol{w}) : [0, 2] \to (-4, 4) \times (-4, 4)$*, i.e.,* $\mathcal{W} = \{\boldsymbol{W}(\cdot, \boldsymbol{w}) : [0, 2] \to (-4, 4) \times (-4, 4) \mid \boldsymbol{w} \in \boldsymbol{\Omega}\}$*, with probability of at least* 0.98*, i.e.,* $\boldsymbol{P}(\{\boldsymbol{w} \in \boldsymbol{\Omega} \mid \boldsymbol{W}(\cdot, \boldsymbol{w}) : [0, 2] \to (-4, 4) \times (-4, 4)\}) \geq 0.98$*. Thus, the set* D *in this case is equal to* $\{\boldsymbol{d} \in \mathbb{R}^2 \mid h_1(\boldsymbol{d}) \geq 0, h_2(\boldsymbol{d}) \geq 0\}$ *with* $h_1(\boldsymbol{d}) = \sin^2 \frac{4}{10} - d_1^2$ *and* $h_2(\boldsymbol{d}) = \sin^2 \frac{4}{10} - d_2^2$*. An inner-approximation* IN *over the time horizon* $[0, 2.0]$*, which is computed via solving* (11)*, is illustrated in Fig. 8–10. The parameters in solving* (11) *are presented in Table VII and the computation time is* 260.58 *seconds.*

d_u	d_{s_1}	d_{s_2}	d_{s_3}	g_R
4	4	4	4	$0.26 - \sum_{i=1}^{7} x_i^2$

TABLE VI

Parameters for solving the semi-definite program (17) *for Example 7.* d_u *denotes the degree of the polynomial* $u(x)$. d_{s_i} *denotes the degree of the sum-of-squares polynomial* s_i, $i = 1, \ldots, 3$.

d_u	d_{s_1}	d_{s_2}	d_{s_3}	d_{s_4}	d_{s_5}	d_{s_6}	R
4	4	4	4	4	4	4	0.26

TABLE VII

Parameters for solving the program (11) *for Example 7.*

Besides we use the time horizon $[0, 2]$ *and the set* $\mathcal{W}$ *of two-dimensional Wiener paths in* $\mathcal{C}^2[0, 2]$ *such that* $\boldsymbol{W}(\cdot, \boldsymbol{w}) : [0, 2] \to \mathbb{R}^2$. *That is, the set* $\mathcal{W} = \{\boldsymbol{W}(\cdot, \boldsymbol{w}) \in \mathcal{C}^2[0, 2] \mid \boldsymbol{w} \in \boldsymbol{\Omega}\}$ *includes the set of all continuous Wiener paths. Its probability measure is 1. Thus, the set* D *in this case is* $\{\boldsymbol{d} \in \mathbb{R}^2 \mid h_1(\boldsymbol{d}) \geq 0, h_2(\boldsymbol{d}) \geq 0\}$ *with* $h_1(\boldsymbol{d}) = 1 - d_1^2$ *and* $h_2(\boldsymbol{d}) = 1 - d_2^2$. *An inner-approximation* IN' *over the time horizon* $[0, 2.0]$, *which is computed via solving* (11), *is illustrated in Fig. 8–10. The parameters in solving* (11) *are presented in Table VII and the computation time is* 288.27 *seconds.*

Similar to Example 6, the comparison results illustrated in Fig. 8–10 imply that the conservativeness in estimating the set of safe initial states of interest can be reduced by considering a smaller subset of Wiener paths. For instance, the set of 0.98*-safe initial states computed based on the set of Wiener paths with probability of at least* 0.98 *is larger than the one computed based on the set of all continuous Wiener paths.*

The scalability of our approach, which reduces stochastic reachability to adversary reachability of ODEs for solving the p-safety problem of RODEs over both finite and infinite time horizons, depends on the underlying reachability techniques for perturbed ODEs. In this paper, the semi-definite programming methods from [43] and [45] are employed to illustrate our approach. The resulting semi-definite program falls within the convex programming framework and can be efficiently solved by interior point methods in polynomial time. Yet the size of the programs (11) and (17) grows extremely fast with the number of state and perturbation variables and the degree of the polynomials occurring in them. Fortunately, the use of template polynomials such as diagonally dominant sum-of-squares (DSOS) and scaled diagonally dominant-sum-of-squares (SDSOS) polynomials [2], which convert the semi-definite programming relaxations into linear programs and second-order cone programs with lower complexity than the semi-definite programs, can enhance the computational efficiency and thus advance scalability of the methods exploiting semi-definite programming.

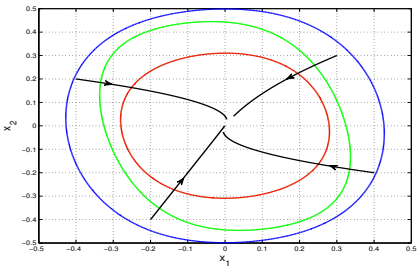

Fig. 8. An illustration of sets of p-safe initial states for Example 7 on the plane $x_1 - x_2$ with $x_3 = x_4 = x_5 = x_6 = x_7 = 0$. The red curve denotes the boundary of the computed robust invariant set $\widetilde{\text{TR}}$. The green curve denotes the boundary of the computed inner-approximation IN' of 0.98-safe initial states. The blue curve denotes the boundary of the computed inner-approximation IN of 0.98-safe initial states. The black curves denote the trajectories of RODE (21) in finite time.

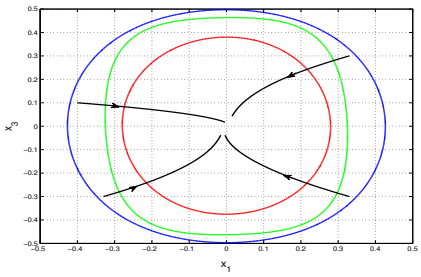

Fig. 9. An illustration of sets of p-safe initial states for Example 7 on the plane $x_1 - x_3$ with $x_2 = x_4 = x_5 = x_6 = x_7 = 0$. The red curve denotes the boundary of the computed robust invariant set $\widetilde{\text{TR}}$. The green curve denotes the boundary of the computed inner-approximation IN' of 0.98-safe initial states. The blue curve denotes the boundary of the computed inner-approximation IN of the 0.98-safe initial states. The black curves denote the trajectories of RODE (21) in finite time.

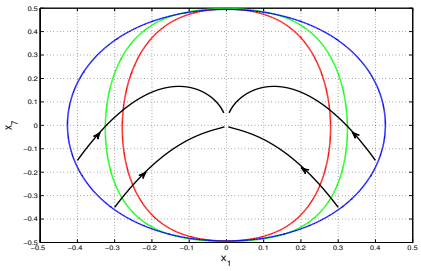

Fig. 10. An illustration of sets of p-safe initial states for Example 7 on the plane $x_1 - x_7$ with $x_2 = x_3 = x_4 = x_5 = x_6 = 0$. The red curve denotes the boundary of the computed robust invariant set $\widetilde{\text{TR}}$. The green curve denotes the boundary of the computed inner-approximation IN' of 0.98-safe initial states. The blue curve denotes the boundary of the computed inner-approximation IN of the 0.98-safe initial states. The black curves denote the trajectories of RODE (21) in finite time.

V. Conclusion

In this paper we studied the safety verification problem for systems modeled by RODEs, which are ODEs that contain stochastic processes. This is the first work on studying the safety verification of RODEs incorporating time-varying stochastic processes. Given a threshold $p \in (0, 1)$, the safety verification problem is to compute a set of initial states such that the probability of the system staying safe is larger than p from each initial state. We considered the safety verification problem over both finite time horizons and the infinite time horizon. Our approach was based on the reduction of stochastic reachability of RODEs to adversary reachability of ODEs, thereby lifting the existing reachability analysis techniques

for perturbed ODEs to RODEs. Finally, we demonstrated our method on several examples.

In this paper we confined ourselves to RODEs incorporating a Wiener process, but the method of reducing stochastic reachability to adversary reachability for ODEs is more generally applicable to RODEs comprising Lévy processes such as a Poisson process. This hinges on the fact that each Lévy process has a measurable modification [3] and that the semi-definite programs (11) *and* (17) *are equally applicable to systems with measurable inputs. One has to furthermore employ Doob's martingale inequality instead of the reflection principle in Alg. 1 to obtain a set of sample paths covering a probability mass of at least p. The remaining procedures stay unaltered.*

In future work we will investigate the conservativeness of our approach and explore more advanced methods for safety verification of RODEs. Also, since RODEs can incorporate bounded noise processes, which reflect the nature of many real physical quantities [9], in our future work we want to apply the proposed safety verification approaches to the safe design of cyber-physical systems such as autonomous vehicles modelled by RODEs with bounded stochastic processes.

REFERENCES

[1] A. Abate, S. Amin, M. Prandini, J. Lygeros, and S. Sastry. Computational approaches to reachability analysis of stochastic hybrid systems. In *HSCC'07*, pages 4–17. Springer, 2007.

[2] A. A. Ahmadi and A. Majumdar. DSOS and SDSOS optimization: more tractable alternatives to sum of squares and semidefinite optimization. *SIAM Journal on Applied Algebra and Geometry*, 3(2):193–230, 2019.

[3] D. Applebaum. *Lévy processes and stochastic calculus*. Cambridge university press, 2009.

[4] L. Arnold. Stochastic Differential Equations. *New York*, 1974.

[5] E. Asarin, T. Dang, and A. Girard. Reachability analysis of nonlinear systems using conservative approximation. In *HSCC'03*, pages 20–35. Springer, 2003.

[6] M. S. Bartlett. *An Introduction to Stochastic Processes: With Special Reference to Methods and Applications*. CUP Archive, 1978.

[7] S. Bogomolov, M. Forets, G. Frehse, F. Viry, A. Podelski, and C. Schilling. Reach set approximation through decomposition with low-dimensional sets and high-dimensional matrices. In *HSCC'18*, pages 41–50. ACM, 2018.

[8] T. Caraballo and R. Colucci. A comparison between random and stochastic modeling for a SIR model. *Communications on Pure & Applied Analysis*, 16(1):151.

[9] A. d'Onofrio. *Bounded Noises in Physics, Biology, and Engineering*. Springer, 2013.

[10] A. Einstein. Über die von der molekularkinetischen theorie der wärme geforderte bewegung von in ruhenden flüssigkeiten suspendierten teilchen. *Annalen der physik*, 322(8):549–560, 1905.

[11] S. Feng, M. Chen, B. Xue, S. Sankaranarayanan, and N. Zhan. Unbounded-time safety verification of stochastic differential dynamics. In *CAV'20*. Springer, 2020.

[12] M. Fränzle, M. Chen, and P. Kröger. In memory of Oded Maler: automatic reachability analysis of hybrid-state automata. *ACM SIGLOG News*, 6(1):19–39, 2019.

[13] M. Fränzle, E. M. Hahn, H. Hermanns, N. Wolovick, and L. Zhang. Measurability and safety verification for stochastic hybrid systems. In *HSCC'11*, pages 43–52. ACM, 2011.

[14] T. Gan, M. Chen, Y. Li, B. Xia, and N. Zhan. Reachability analysis for solvable dynamical systems. *IEEE Transactions on Automatic Control*, 63(7):2003–2018, 2017.

[15] E. Goubault, S. Putot, and L. Sahlmann. Inner and outer approximating flowpipes for delay differential equations. In *CAV'18*, pages 523–541. Springer, 2018.

[16] X. Han and P. E. Kloeden. *Random Ordinary Differential Equations and Their Numerical Solution*. Springer, 2017.

[17] P. Holmes, S. Kousik, S. Mohan, and R. Vasudevan. Convex estimation of the α-confidence reachable set for systems with parametric uncertainty. In *CDC'16*, pages 4097–4103. IEEE, 2016.

[18] J. Hu, J. Lygeros, and S. Sastry. Towards a theory of stochastic hybrid systems. In *HSCC'00*, pages 160–173. Springer, 2000.

[19] C. Huang, X. Chen, W. Lin, Z. Yang, and X. Li. Probabilistic safety verification of stochastic hybrid systems using barrier certificates. *ACM Transactions on Embedded Computing Systems (TECS)*, 16(5s):186, 2017.

[20] I. Karatzas and S. E. Shreve. *Brownian Motion and Stochastic Calculus*. Springer Verlag, New York, 1988.

[21] X. D. Koutsoukos and D. Riley. Computational methods for verification of stochastic hybrid systems. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 38(2):385–396, 2008.

[22] K. Liu, M. Li, and Z. She. Reachability estimation of stochastic dynamical systems by semi-definite programming. In *CDC'19*, pages 7727–7732. IEEE, 2019.

[23] P. Mörters and Y. Peres. *Brownian motion*, volume 30. Cambridge University Press, 2010.

[24] T. Neckel and F. Rupp. *Random differential equations in scientific computing*. Walter de Gruyter, 2013.

[25] B. Øksendal. Stochastic differential equations. In *Stochastic differential equations*, pages 65–84. Springer, 2003.

[26] A. Platzer. Stochastic differential dynamic logic for stochastic hybrid programs. In *CADE'11*, pages 446–460. Springer, 2011.

[27] G. Pola, M. L. Bujorianu, J. Lygeros, and M. D. Di Benedetto. Stochastic hybrid models: An overview. *IFAC Proceedings Volumes*, 36(6):45–50, 2003.

[28] S. Prajna, A. Jadbabaie, and G. J. Pappas. Stochastic safety verification using barrier certificates. In *CDC'04*, volume 1, pages 929–934. IEEE, 2004.

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

[30] P. E. Protter. Stochastic differential equations. In *Stochastic integration and differential equations*, pages 249–361. Springer, 2005.

[31] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic. Cyber-physical systems: the next computing revolution. In *Design Automation Conference*, pages 731–736. IEEE, 2010.

[32] N. Ramdani, N. Meslem, and Y. Candau. A hybrid bounding method for computing an over-approximation for the reachable set of uncertain nonlinear systems. *IEEE Transactions on Automatic Control*, 54(10):2352–2364, 2009.

[33] J. Roger et al. *The life sciences in eighteenth-century French thought*. Stanford University Press, 1997.

[34] S. Särkkä and A. Solin. *Applied stochastic differential equations*, volume 10. Cambridge University Press, 2019.

[35] F. Shmarov and P. Zuliani. Probreach: verified probabilistic delta-reachability for stochastic hybrid systems. In *HSCC'15*, pages 134–139. ACM, 2015.

[36] S. E. Z. Soudjani, R. Majumdar, and A. Abate. Safety verification of continuous-space pure jump Markov processes. In *TACAS'16*, pages 147–163. Springer, 2016.

[37] J. Strand. Random ordinary differential equations. *Journal of Differential Equations*, 7(3):538–553, 1970.

[38] D. W. Stroock and S. S. Varadhan. *Multidimensional Diffusion Processes*. Springer, 2007.

[39] C. J. Tomlin, J. Lygeros, and S. S. Sastry. A game theoretic approach to controller design for hybrid systems. *Proceedings of the IEEE*, 88(7):949–970, 2000.

[40] M. Von Smoluchowski. Zur kinetischen theorie der brownschen molekularbewegung und der suspensionen. *Annalen der physik*, 326(14):756–780, 1906.

[41] S. Wang, N. Zhan, and L. Zhang. A compositional modelling and verification framework for stochastic hybrid systems. *Formal Asp. Comput.*, 29(4):751–775, 2017.

[42] R. Wisniewski, C. Sloth, M. Bujorianu, and N. Piterman. Safety verification of piecewise-deterministic markov processes. In *HSCC'16*, pages 257–266. ACM, 2016.

[43] B. Xue, M. Fränzle, and N. Zhan. Inner-approximating reachable sets for polynomial systems with time-varying uncertainties. *IEEE Transactions on Automatic Control*, 65(4):1468–1483, 2020.

[44] B. Xue, Z. She, and A. Easwaran. Under-approximating backward reachable sets by polytopes. In *CAV'16*, pages 457–476. Springer, 2016.

[45] B. Xue, Q. Wang, N. Zhan, and M. Fränzle. Robust invariant sets generation for state-constrained perturbed polynomial systems. In *HSCC'19*, pages 128–137. ACM, 2019.

[46] L. Zhang, Z. She, S. Ratschan, H. Hermanns, and E. M. Hahn. Safety verification for probabilistic hybrid systems. In *CAV'10*, pages 196–211. Springer, 2010.