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

Christian 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 sub-phomena 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:

$$X(t) = X(t_0) + \int_{t_0}^{t} a(s, X(s))ds + \sum_{i=1}^{n} \sigma(s_{i-1}, X(s_{i-1}))(W(s_i) - W(s_{i-1}))$$  \hspace{1cm} (1)
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:

\[
\frac{dx}{dt} = f(x, Y(t)),
\]

where \( Y(t) \) 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 [22], 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 [11] we introduce Wiener processes, RODEs and the \( p \)-safety problem. Section [11] 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, \( C^k[0,T] \) denotes the space of continuous functions mapping \([0,T] \) into \( \mathbb{R}^k \), \( C^k[0,\infty) \) 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 \((\Omega, \mathcal{F}, \mathbb{P})\). Let \( \mathcal{F} = \sigma(\{W_s \mid s \leq t\}) \), \( \mathcal{F}_t\) be a filtration defined on it. A process \( \{W(t, w) : \mathbb{R}_+ \times \Omega \to \mathbb{R}\} \) is said to be a 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 \( \sigma^2(s - t) > 0 \) for all \( s, t \geq 0 \); and
4) the sample path \( W(\cdot, w) : [0, \infty) \to \mathbb{R} \) is in \( C^1[0,\infty) \).

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 \( \mathcal{F}_t\) is simply a natural filtration, i.e., \( \mathcal{F}_s = \sigma(\{W_s \mid 0 \leq s \leq t\}) \), 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 \textit{absolute value} at the terminal time.

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

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

\[ P(\{ w \in \Omega \mid S_t \leq b \}) = P(\{ w \in \Omega \mid |W(t, w)| \geq -b \}) = \frac{2}{\sqrt{2\pi b^2 t}} \int_{-\infty}^b e^{-\frac{x^2}{2b^2 t}} dx, \]

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

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 \((\Omega_i, \mathcal{F}_i, \mathbb{P}_i)\). For convenience, we denote the \( m \) Wiener processes \( \{W_i(\cdot, \cdot) \mid i = 0, \ldots, m\} \) by \( W(\cdot, \cdot) \), which maps from \([0, \infty) \) to \( \mathbb{R}^m \), and its probability space by \((\Omega, \mathcal{F}, \mathbb{P})\).

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

\[ P(\{ w \in \Omega \mid S_{i,t} \geq a_i \}) = \prod_{i=1}^m P(\{ w_i \in \Omega_i \mid S_{i,t} \geq a_i \}), \]

where \( w = (w_1, \ldots, w_m) \) 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:

\[ \dot{x}(s) = f(x(s), W(s, w)), \]

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

We assume in what follows that the vector field \( f : \mathbb{R}^n \to \mathbb{R}^n \) satisfies the following two conditions:

1) \( f(x, d) \) is continuous over \( x \in \mathbb{R}^n \) and \( d \in \mathbb{R}^m \);
2) for each \( d \in \mathbb{R}^m \), \( f(x, d) \) is locally Lipschitz continuous over \( x \), i.e., for each \( d \in \mathbb{R}^m \) and each compact set \( X \) in \( \mathbb{R}^n \), there is some constant \( L \) such that

\[ ||f(x, d) - f(z, d)|| \leq L||x - z||, \forall x, z \in X, \]

where \( || \cdot || \) denotes the usual Euclidean norm.

Consequently, according to [16], for the Wiener path \( W(\cdot, \cdot) : [0, \infty) \to \mathbb{R}^m \), there exists a unique continuously differentiable solution to (4) for some time interval. We denote the unique solution as \( \phi_W(x_0) \) with \( \phi_W(x_0) = x_0 \).

Given a safe set \( S = \{ x \in \mathbb{R}^n \mid g(x) \leq 0 \} \) with \( g(\cdot) : \mathbb{R}^n \to \mathbb{R} \) and a target set \( TR = \{ x \in \mathbb{R}^n \mid t(x) \leq 0 \} \) with \( t(\cdot) : \mathbb{R}^n \to \mathbb{R} \), 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 \( x_0 \) is \( p \)-safe.

1) for a finite time horizon \([0, T]\) iff the probability that the induced trajectories of system (4) starting from \( x_0 \) reach the target set \( TR \) at time instant \( t = T \) while staying within the safe set \( S \) over the time horizon \([0, T]\) is larger than \( p \), i.e.,

\[ P\left( \left\{ w \in \Omega \mid \forall s \in [0, T], \phi_W(x_0)(s) \in X, \phi_W(x_0)(T) \in TR \right\} \right) \geq p, \]

where \( T \in (0, \infty) \).
2) for the infinite time horizon iff the probability that the induced trajectories of system \( f \) starting from \( x_0 \) stay within the safe set \( X \) over the infinite time horizon \([0, \infty)\) is larger than \( p \), i.e.,

\[
P(\{w \in \Omega \mid \forall s \in [0, \infty), \phi^{W_w}(s) \in X\}) \geq p.
\]

The \( p \)-safety problem is to identify a set of \( p \)-safe initial states \( x_0 \) 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.,

\[
P(\{w \in \Omega \mid W(t, w) \in D, \forall t \in [0, T]\}) \geq p,
\]

and \( D \) is the set of continuous functions mapping \([0, T]\) to \( D \), i.e., \( D = \{d(\cdot) \in C^m([0, T]) \mid d(t) \in D, \forall t \in [0, T]\} \). If \( IN \) is an inner approximation of the robust backward reachable set for perturbed ODE (5) over the time horizon \([0, T]\), with

\[
x(s) = f(x(s), d(s)), s \in [0, T],
\]

where \( d(\cdot) \in D \) 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 \( d(\cdot) : [0, T] \to D \) and the initial state \( x_0 \) by \( \psi_{x_0}^{d(\cdot)} : [0, T] \to \mathbb{R}^n \). Therefore, the robust backward reachable set for perturbed ODE (5) is \( \{x_0 \in \mathbb{R}^n \mid \forall t \in [0, T], \forall d(\cdot) \in D, x_0(\cdot) \in X \wedge \psi_{x_0}^{d(\cdot)}(T) \in TR\} \), denoted by \( R^m \). Clearly, \( IN \subseteq R^m \).

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 \( W \). Obviously, \( W \subseteq D \).

For \( x_0 \in IN \), we have that

\[
P(\{w \in \Omega \mid \forall t \in [0, T], \phi_{x_0}^{W_w}(t) \in X \wedge \phi_{x_0}^{W_w}(T) \in TR\}) \geq A + B \geq A,
\]

where

\[
A = P(\{w \in \Omega \mid \forall s \in [0, T], W(s, w) \in W \wedge \phi_{x_0}^{W_w}(s) \in X \wedge \phi_{x_0}^{W_w}(T) \in TR\})
\]

and

\[
B = P(\{w \in \Omega \mid \forall s \in [0, T], W(s, w) \notin W \wedge \phi_{x_0}^{W_w}(s) \in X \wedge \phi_{x_0}^{W_w}(T) \notin TR\}).
\]

Moreover, since \( W \subseteq D \), \( W(s, w) \in D \) if \( W(s, w) \in W \). Likewise, as \( \phi_{x_0}^{W_w}(s) = \psi_{x_0}^{W_w}(s) \) for \( s \in [0, T] \), it follows \( \phi_{x_0}^{W_w}(s) \in X \) for \( s \in [0, T] \) and \( \phi_{x_0}^{W_w}(T) \in TR \) if \( W(s, w) \in W \). Thus,

\[
P(\{w \in \Omega \mid \forall s \in [0, T], W(s, w) \in W \wedge \phi_{x_0}^{W_w}(s) \in X \wedge \phi_{x_0}^{W_w}(T) \in TR\}) = P(\{w \in \Omega \mid W(s, w) \in W\}) \geq p.
\]

Hence, \( P(\{w \in \Omega \mid \forall s \in [0, T], \phi_{x_0}^{W_w}(s) \in X \wedge \phi_{x_0}^{W_w}(T) \in TR\}) \geq p \). Definition 3 indicates that \( x_0 \) 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 \( W \) 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 \( W \) 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,
\[ \dot{x}(s) = -x(s) + 10 \sin \left( \frac{W(s,w)}{10} \right) x^3(s), s \in [0, T], \]  
(6)
where \( T = 1, X = \{x \in \mathbb{R} | g(x) \leq 0\} \) with \( g(x) = x^2 - 0.9 \), \( TR = \{x \in \mathbb{R} | l(x) \leq 0\} \) 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 - 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 - 10^{-6}, i.e.,
\[ P(\{w \in \Omega \mid W(\cdot, w) \in \mathcal{W}\}) \geq 1 - 10^{-6}. \]

This is done as follows: Since
\[ P(\{w \in \Omega \mid W(t, w) \in (b, a), \forall t \in [0, 1]\}) \]
\[ = P(\{w \in \Omega \mid W(t, w) \in (\tau_a \wedge \tau_b, \tau_a \wedge \tau_b) \} \cap \{w \in \Omega \mid \tau_a \wedge \tau_b \leq 1\}) \]
\[ = 1 - P(\{w \in \Omega \mid \tau_a \wedge \tau_b \geq 1\}) \]
(7)
where \( a > 0 \) and \( b < 0 \), \( \tau_a = \inf\{s \in [0, \infty) \mid W(s, w) \geq a\} \), \( \tau_b = \inf\{s \in [0, \infty) \mid W(s, w) \leq b\} \), \( \tau_a \wedge \tau_b = \max\{\tau_a, \tau_b\} \),
\[ P(\{w \in \Omega \mid W(t, w) \in (b, a), \forall t \in [0, 1]\}) \]
\[ \geq 1 - P(\{w \in \Omega \mid \tau_a \wedge \tau_b \leq 1\}) \]
holds. According to the reflection principle in Theorem 1, we have
\[ P(\{w \in \Omega \mid \tau_a \leq 1\}) \]
\[ = P(\{w \in \Omega \mid |W(1, w)| \geq a\}) = 2 - \frac{1}{\sqrt{2\pi}} \int_a^\infty e^{-\frac{x^2}{2}} dx \]
and
\[ P(\{w \in \Omega \mid \tau_b \leq 1\}) \]
\[ = P(\{w \in \Omega \mid |W(1, w)| \leq b\}) = 2 - \frac{1}{\sqrt{2\pi}} \int_b^\infty e^{-\frac{x^2}{2}} dx. \]
Therefore, we just need to solve the following optimization problem:
\[ \min a - b \]
\[ \text{s.t.} \ 1 - 2 - \frac{1}{\sqrt{2\pi}} \int_a^\infty e^{-\frac{x^2}{2}} dx 
- 2\frac{1}{\sqrt{2\pi}} \int_b^\infty e^{-\frac{x^2}{2}} dx 
\geq 1 - 10^{-6} \]
\[ a \geq 0, b \leq 0. \]
(8)
The objective function \( a - b \) corresponds to the Lebesgue measure of the set \( D \). Since
\[ 1 - 2 - \frac{1}{\sqrt{2\pi}} \int_a^\infty e^{-\frac{x^2}{2}} dx - 2\frac{1}{\sqrt{2\pi}} \int_b^\infty e^{-\frac{x^2}{2}} dx = 1 - 2\frac{1}{\sqrt{2\pi}} \int_a^\infty e^{-\frac{x^2}{2}} dx - 2\frac{1}{\sqrt{2\pi}} \int_0^\infty e^{-\frac{x^2}{2}} dx \]
is monotonically increasing over \( a \) and monotonically decreasing over \( b \), the simplest approach for solving the optimization \( \text{[8]} \) is linear search. Via solving \( \text{[8]} \) based on linear search, we obtain \( a = -b = 5.0 \).

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Parameter</th>
<th>Value</th>
<th>Parameter</th>
<th>Value</th>
<th>Parameter</th>
<th>Value</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>( d_{a1} )</td>
<td>10</td>
<td>( d_{a2} )</td>
<td>10</td>
<td>( d_{a3} )</td>
<td>10</td>
<td>( d_{a4} )</td>
<td>10</td>
<td>( d_{a5} )</td>
<td>10</td>
</tr>
<tr>
<td>( R )</td>
<td>1</td>
<td>( d_{a1} )</td>
<td>10</td>
<td>( d_{a2} )</td>
<td>10</td>
<td>( d_{a3} )</td>
<td>10</td>
<td>( d_{a4} )</td>
<td>10</td>
</tr>
</tbody>
</table>

Step 2 of Alg. 1. By regarding the Wiener paths \( W(\cdot, w) \) in \( W \) as perturbation inputs, we consider the perturbed ODE:
\[ \dot{x}(s) = -x(s) + 10 \sin \left( \frac{d(s)}{10} \right) x^3(s), s \in [0, T], \]
(9)
where \( T = 1, X = \{x \in \mathbb{R} | g(x) \leq 0\} \), \( TR = \{x \in \mathbb{R} | l(x) \leq 0\} \), \( d(\cdot) : [0, 1] \to (-5, 5) \) is the continuous perturbation input. Since \( \sin^2 \) is monotonically increasing over \( d \in (-5, 5) \), we further relax [9] to [10] \[ \dot{x}(s) = -x(s) + 10d(s)x^3(s), s \in [0, T], \]
(10)
where \( T = 1, X = \{x \in \mathbb{R} | g(x) \leq 0\} \), \( TR = \{x \in \mathbb{R} | l(x) \leq 0\} \), \( d(\cdot) : [0, 1] \to [-\sin^2 \frac{\pi}{2}, \sin^2 \frac{\pi}{2}] \) is the continuous perturbation input and \( D = \{d \in \mathbb{R} | |d| \geq 0\} \) with \( |d| = \sin^2 \frac{\pi}{2} - d^2 \). Clearly, the trajectories of Eq. 10[10] include the ones of Eq. 9[9].

Step 3 of Alg. 1. From [23], an inner approximation of the robust backward reachable set \( \text{IN} = \{x \mid u(x, 0) \leq 0\} \) for ODE [10] can be computed by solving the semi-definite program [11]:
\[ \inf e^T \cdot m \]
\[ \text{s.t.} \quad -Lu(x, t) - s_1gR(x) - s_2t(T - t) - s_3h(d) = \sum_i [x, t, d], \]
\[ u(x, t) - g(x) - s_4gR(x) - s_5t(T - t) = \sum_i [x, t], \]
\[ u(x, T) - t(x) - s_6gR(x) \in \sum_i [x], \]
(11)

where \( e^T \cdot m = \int_{B_R} u(x, 0) dx \), \( m \) 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 \( c \) is expressed, and \( Lu(x, t) = \partial_t u(x, t) + \nabla u(x, t) \cdot (-x + 10dx^3) \), \( B_R = \{x \in \mathbb{R} | g(x) \geq 0\} \), where \( g(x) \) is \( R - x^2 \) with \( R \) being a positive number such that \( X \subseteq B_R \) and \( \partial X \cap \partial B_R = \emptyset \). \( \sum_i [\cdot] \) 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 \( \text{IN} = \{x \in B_R \mid u(x, 0) \leq 0\} \), which is illustrated in Fig. 1. The computation time is 45.68 seconds on an i7-7500U 2.70GHz CPU with 32GB RAM running Windows 10. According to Theorem 2, every initial state in \( \text{IN} \) for RODE \text{[6]} \( (1 - 10^{-6}) \)-safe. The parameters for solving \text{[11]} are presented in Table 1.

In Example \text{[1]} the semi-definite programming based method \text{[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., \( f(x, d) \in \mathbb{R}[x, d], g(x) \in \mathbb{R}[x], l(x) \in \mathbb{R}[x] \) and \( h(d) \in \mathbb{R}[d] \). Actually, any existing (inner-approximate) reachability techniques for
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 \( W \) of Wiener paths staying within a bounded set and having probability of at least \( p \) is not unique. However, the set \( W \) 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 \( f(x, W(s, w)) \) satisfying

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

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 II-A to compute an inner approximation of the robust backward reachable set, therefore expanding the set of \( p \)-safe initial states. Every state \( x_0 \) 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., \( P(\{w \in \Omega \mid \forall s \in [0, \tau], W(s, w) \in D\}) \geq p \). \( D \) is the set of continuous functions mapping \([0, \tau]\) to \( D \), i.e., \( D = \{d(\cdot) \in C^m[0, \tau] \mid d(\cdot) : [0, \tau] \to D\} \). If \( IN \) is a set of initial states from which all trajectories to ODE (12) enter the target set \( TR \) at time \( t = \tau \) while staying within the safe state set \( X \) over the time horizon \([0, \tau]\), where \( TR \) is a robust invariant set for ODE (13) such that all trajectories starting from it stay within the safe state set \( X \) forever, where

\[
\dot{x}(s) = f(x(s), d(s)),
\]

with \( d(\cdot) \in D \) being the perturbation input, and

\[
\dot{x}(s) = f(x(s), d'(s)),
\]

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

**Proof.** We denote the trajectory to ODE (12) with the perturbation input \( d(\cdot) : [0, \tau] \to D \) and the initial state \( x_0 \) by \( \phi^{d(x_0)}_{\tau}(\cdot) : [0, \tau] \to \mathbb{R}^n \). 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 \( W \). Clearly, \( W \subseteq D \). We denote the trajectory to ODE (13) with the perturbation input \( d'(\cdot) : [0, \infty) \to \mathbb{R}^m \) and the initial state \( x_0 \) by \( \phi^{d'(x_0)}_{\tau}(\cdot) \).

Since \( \phi^{W(x_0)}_{\tau}(s) = \phi^{W(x_0)}_{\tau}(s) \) for \( W(\cdot, w) \in C^m[0, \infty) \) and \( t \in [0, \tau) \), we have that if \( x_0 \in TR \),

\[
P(\{w \in \Omega \mid \forall s \in [0, \infty), \phi^{W(x_0)}_{\tau}(s) \in X\}) = P(\{w \in \Omega \mid W(\cdot, w) \in C^m[0, \infty)\}) = 1 \geq p.
\]

If \( x_0 \in IN \), we have that

\[
P(\{w \in \Omega \mid \forall s \in [0, \tau], \phi^{W(x_0)}_{\tau}(s) \in X\}) \geq P\left(\{w \in \Omega \mid \forall s \in [0, \tau], \phi^{W(x_0)}_{\tau}(s) \in X \land \phi^{W(x_0)}_{\tau}(\tau) \in TR\}\right) = A + B \geq A,
\]

where

\[
A = P\left(\left\{w \in \Omega \mid \forall s \in [0, \tau], W(\cdot, w) \in D \land \phi^{W(x_0)}_{\tau}(s) \in X \land \phi^{W(x_0)}_{\tau}(\tau) \in TR\right\}\right)
\]

and
and
\[ B = P \left\{ w \in \Omega \left| \forall s \in [0, \tau], W(\cdot, w) \notin D \cap \phi_{x_0}^W(s) \in X \wedge \phi_{x_0}^W(\tau) \in \widetilde{TR} \right. \right\}. \]

Since \( W \subseteq D \), \( W(\cdot, w) \in D \) if \( W(\cdot, w) \in W \). Also, since \( \phi_{x_0}^W(s) = \psi_{x_0}^W(s) \) for \( s \in [0, \tau] \),
\[ P \left\{ w \in \Omega \left| \forall s \in [0, \tau], W(\cdot, w) \in D \cap \phi_{x_0}^W(s) \in X \wedge \phi_{x_0}^W(\tau) \in \widetilde{TR} \right. \right\} = P \left\{ w \in \Omega \left| W(\cdot, w) \in D \right. \right\} \geq p. \]

Consequently, \( P \left\{ w \in \Omega \left| \forall s \in [0, \tau], \phi_{x_0}^W(s) \in X \right. \right\} \geq p \). Definition \ref{def:p-safe} indicates that \( x_0 \in \text{IN} \cup \text{TR} \) is \( p \)-safe.

Reflecting the constructions from the proof of Theorem \ref{thm:p-safe}, our method for solving \( p \)-safety problem over the infinite time horizon is summarized in Alg. \ref{alg:framework}.

**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 (\ref{eq:RODE}); 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 (\ref{eq:perturbed ODE}) 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 \( \text{TR} \);
3. Choose a finite time horizon \([0, \tau] \);
4. Obtain an inner approximation IN by applying Alg. \ref{alg:invariant set generation} to RODE (\ref{eq:RODE}) with the safe set \( X \), target set TR, time horizon \([0, \tau] \) and safety level \( p \);
5. Return the set \( \text{IN} \cup \text{TR} \), 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 (\ref{eq:perturbed ODE}) and (\ref{eq:perturbed ODE 2}) in Alg. \ref{alg:framework} can be further relaxed into another perturbed ODEs, which are relatively easily manipulated with their trajectories including the ones of ODEs (\ref{eq:perturbed ODE}) and (\ref{eq:perturbed ODE 2}) 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,
\[ \dot{x}(s) = -x(s) + 0.09x^2(s) + 0.5 \sin(\frac{W(s, \mu)}{10})x^3(s) \] \tag{15}
with \( X = \{ x \in \mathbb{R} \mid g(x) \leq 0 \} \) with \( g(x) = x^2 - 2 \), and the stochastic process \( W(s, \mu) : [0, \infty) \times \Omega \rightarrow \mathbb{R} \) 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. \ref{alg:framework} since \( \sin(\cdot) : \mathbb{R} \rightarrow [-1, 1] \), by regarding \( \sin(\frac{W(s, \mu)}{10}) : [0, \infty) \times \Omega \rightarrow [-1, 1] \) as perturbation inputs \( d(\cdot) : [0, \infty) \rightarrow [-1, 1] \), we consider the perturbed ODE
\[ \dot{x}(s) = -x(s) + 0.09x^2(s) + 0.5d(s)x^3(s) \] \tag{16}
\( \text{TABLE II} \)

<table>
<thead>
<tr>
<th>( d_{u1} )</th>
<th>( d_{u2} )</th>
<th>( d_{u3} )</th>
<th>( g_R )</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>8</td>
<td>8</td>
<td>2.1 - x^2</td>
</tr>
</tbody>
</table>

\( \text{Parameters for solving the semi-definite program (17) for Example 2} \)

\( d_u \) denotes the degree of the polynomial \( u(x) \). \( d_{u1} \) denotes the degree of the sum-of-squares polynomial \( s_i = 1, \ldots, 3 \). \( g_R \) is the constant term.

where \( X = \{ x \in \mathbb{R} \mid g(x) \leq 0 \} \) and \( d(\cdot) : [0, \infty) \rightarrow D \) 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) includes the ones of (15).

Step 2 of Alg. \ref{alg:framework} 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 \( d(\cdot) : [0, \infty) \rightarrow D \). From (15), a robust invariant set \( R = \{ x \in X \mid u(x) \leq 0 \} \) of perturbed ODE (16) could be computed by solving the semi-definite program (17):
\[ \inf c^T \cdot m \]
s.t.
\[ -Lu(x) - s_1h(d) - s_2g_R(x) \in \mathbb{R}, \quad 1 + g^2(x)u(x) - g(x) - s_3g_R(x) \in \mathbb{R}. \] \tag{17}
\( c^T \cdot m = \int_{B_R} u(x)dx \) is the vector composed of unknown coefficients in \( u(x) \in \mathbb{R}[x] \). \( m \) is the constant vector computed by integrating the monomials in \( u(x) \) over \( B_R \). \( B_R \) is the set \( \{ x \in \mathbb{R} \mid g_R(x) \geq 0 \} \) with \( g_R(x) \in \mathbb{R}[x] \) such that \( X \subseteq B_R \) and \( \partial X \cap \partial B_R = \emptyset \), and \( Lu(x) = \nabla_x u(x) \cdot (-x + 0.09x^2 + 0.5dx^3) \). \( \sum \) denotes the set of sum-of-squares polynomials over the argument. The minimum is over the polynomial \( u(x) \) and sum-of-squares polynomials \( s_1(x, d), s_2(x, d), s_3(x) \).

The computed robust invariant set \( \widetilde{TR} = \{ x \in B_R \mid u(x) \leq 0 \} \) 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. \ref{alg:framework} We choose the time horizon \([0, \tau] \) with \( \tau = 1 \).

Step 4 of Alg. \ref{alg:framework} Via taking the computed robust invariant set \( \widetilde{TR} = \{ x \in B_R \mid u(x) \leq 0 \} \) as the target set, we further compute a set \( \text{IN} \) of \( p \)-safe initial states such that
\[ P \left\{ w \in \Omega \left| \forall s \in [0, \tau], \phi_{x_0}^W(s) \in X \wedge \phi_{x_0}^W(\tau) \in \widetilde{TR} \right. \right\} \geq p, \]
where \( \tau = 1 \). Like Example 2 we first identify a set \( W \) of Wiener paths. Since \( p = 1 \), therefore, we use all of Wiener paths. That is, \( W = \{ W(\cdot, w) \in C^1[0, \tau] \mid w \in \Omega \} \). The probability \( P \left\{ w \in \Omega \mid W(\cdot, w) \in W \right. \right\} \) is equal to 1. An inner-approximation IN is \( \{ x \in B_R \mid u(x, 0) \leq 0 \} \), which is also illustrated in Fig. 2 of the robust backward reachable set for ODE (16) with \( d(\cdot) : [0, 1] \rightarrow D \) is obtained by solving (15). The parameters in solving (15) are presented in Table II. The computation time is 31.35 seconds.

Step 5 of Alg. \ref{alg:framework} We obtain a set \( \text{IN} \cup \widetilde{TR} \). According to Theorem \ref{thm:invariant set}, every state in \( \text{IN} \cup \widetilde{TR} \) is 1-safe for RODE (15).
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 \cite{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 $\tau$ 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 $\tau$ in future work.

IV. Experiments

In this section we illustrate our approach on five examples based on solving the programs \cite{11} and \cite{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 2.70GHz 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 \cite{6} described in Example 7 again. In this example the computed set of p-safe initial states over finite time horizons.

We first use the set $W$ of all Wiener paths $W(\cdot,w) : [0,T] \rightarrow (-\infty,\infty)$ to attempt computing a set of 1-safe initial states. That is, $W = \{W(\cdot,w) : [0,T] \rightarrow (-\infty,\infty) \mid w \in \Omega\}$ and $P(\{w \in \Omega \mid W(\cdot,w) \in W\}) = 1$. 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 2 we obtain an empty set of 1-safe initial states, which is a correct but useless inner approximation.

Then we use the set $W$ of Wiener paths $W(\cdot,w) : [0,T] \rightarrow (-2,2)$. That is, $W = \{W(\cdot,w) : [0,T] \rightarrow (-2,2) \mid w \in \Omega\}$. Its probability is larger than 0.9, i.e., $P(\{w \in \Omega \mid W(\cdot,w) : [0,T] \rightarrow (-2,2)\}) \geq 0.9$. Thus, the set $D$ in (16) is equal to $\{d \in \mathbb{R} \mid h(d) \geq 0\}$ with $h(d) = \sin^2 \frac{\pi d}{36} - d^2$. Via solving the semi-definite program (11) with the parameters listed in Table 2 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 $W$ of Wiener paths $W(\cdot,w) : [0,T] \rightarrow (-1,1)$. Its probability is larger than 0.36, i.e., $P(\{w \in \Omega \mid W(\cdot,w) : [0,T] \rightarrow (-1,1)\}) \geq 0.36$. Thus, the set $D$ in (16) is equal to $\{d \in \mathbb{R} \mid h(d) \geq 0\}$ with $h(d) = \sin^2 \frac{\pi d}{36} - d^2$. Via solving the semi-definite program (11) with the parameters listed in Table 2 we obtain a set of 0.36-safe initial states, which is illustrated in Fig. 3. The computational 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 \cite{25}:

\[
\dot{x}(s) + a_0 \dot{x}(s) + \beta^2 x(s) = (T_0 - a_0 \dot{x}(s))\eta W(s,w),
\]

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

\[
\begin{align*}
\dot{x}(s) &= y(s) \\
\dot{y}(s) &= -a_0 y(s) - \beta^2 x(s) + (T_0 - a_0 y(s))\eta W(s,w),
\end{align*}
\]

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

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 $W$ of Wiener paths $W(\cdot,w) : [0,T] \rightarrow (-2,2)$, i.e., $W = \{W(\cdot,w) : [0,T] \rightarrow (-2,2) \mid w \in \Omega\}$. Its probability is at least 0.90, i.e., $P(\{w \in \Omega \mid W(\cdot,w) : [0,T] \rightarrow (-2,2)\}) \geq 0.9$. 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 4 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
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 $[0,T]$.

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

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 $[0,T]$.

### Example 5

The dynamics of a car in the two dimensions $(x_1, x_2)^T$ of the plane are governed by Newton’s law:

$$f(t) = m \ddot{x}(t),$$

where $\alpha(t)$ is the acceleration (in vectorial form), $m$ is the mass of the car, and $f(t)$ is a vector of (unknown) forces acting on the car. Let us model $\frac{f(t)}{m}$ as a two-dimensional Wiener process $\{\xi_1, \xi_2\}$:

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

which can be written as a first-order RODE:

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

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

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

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

In this model $W(\cdot, \cdot) = (W_1(\cdot, \cdot), W_2(\cdot, \cdot))^T$ 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 $W$ of Wiener paths $W(\cdot, w) : [0, T] \to (-0.01, 0.01) \times (-0.01, 0.01)$, i.e., $W = \{W(\cdot, w) : [0, T] \to (-0.01, 0.01) \times (-0.01, 0.01) \mid w \in \Omega\}$, where probability mass of at least 0.8, i.e., $P\{w \in \Omega \mid W(\cdot, w) : [0, T] \to (-0.01, 0.01) \times (-0.01, 0.01)\} \geq 0.8.$

Thus, the set $D$ in this example is equal to $\{d \in \mathbb{R}^2 \mid h_1(d) \geq 0, h_2(d) \geq 0\}$ with $h_1(d) = 0.01^2 - d_1^2$ and $h_2(d) = 0.01^2 - d_2^2$. Via solving the semi-definite program (21) 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.

### B. Safety Verification over the Infinite Time Horizon

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

### Table IV

<table>
<thead>
<tr>
<th>$a_1$</th>
<th>$a_2$</th>
<th>$a_3$</th>
<th>$a_4$</th>
<th>$a_5$</th>
<th>$a_6$</th>
<th>$b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>2.1</td>
<td>2.1</td>
<td>2.1</td>
<td>2.1</td>
<td>2.1</td>
<td>2.1</td>
</tr>
</tbody>
</table>

### Table V

<table>
<thead>
<tr>
<th>$a_1$</th>
<th>$a_2$</th>
<th>$a_3$</th>
<th>$a_4$</th>
<th>$a_5$</th>
<th>$a_6$</th>
<th>$b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>1.1</td>
<td>1.1</td>
<td>1.1</td>
<td>1.1</td>
<td>1.1</td>
<td>1.1</td>
</tr>
</tbody>
</table>
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 $(1 − 1.2 \times 10^{-6})$-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 $\mathcal{T}\mathcal{R}$ computed in Example 2. Then we first choose the time horizon $[0,1.5]$ and the set $\mathcal{W}$ of Wiener paths in $C[0,\infty)$ such that $W(\cdot,\omega) : [0,1.5] \to \mathbb{R}$. That is, $\mathcal{W} = \{ W(\cdot,\omega) \in C[0,1.5] \mid \omega \in \Omega \}$ includes the set of all continuous Wiener paths. Its probability measure is $\nu$. 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 $C[0,\infty)$ such that $W(\cdot,\omega) : [0,1] \to (-5,5)$. That is, $\mathcal{W} = \{ W(\cdot,\omega) \in C[0,1] \mid \omega \in \Omega \}$. 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 $h(d) = \sin^2 \frac{\pi}{5} - d^2$. 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 $(1−1.2\times10^{-6})$-safe initial states computed based on the set of continuous Wiener paths with a probability of at least $(1−1.2\times10^{-6})$ 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,

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

where $X = \{ x \in \mathbb{R}^7 : g(x) \leq 0 \}$, $g(x) = \sum_{i=1}^{7} x_i^2 - 0.25$ and the stochastic process $W(\cdot,\cdot) = (W_1(\cdot,\cdot),W_2(\cdot,\cdot))^T$ being a 2-dimensional standard Wiener process. The p-safe 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

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

where $X = \{ x \in \mathbb{R}^7 : g(x) \leq 0 \}$, $d_1(\cdot) : [0,\infty) \to [−1,1]^2$. Via solving the semi-definite program (17), we obtain a robust invariant set $\mathcal{T}\mathcal{R} = \{ x \in B_R \mid u(x) \leq 0 \}$ for ODE (21), which is illustrated in Fig. 8. Obviously, it is a set of 1-safe initial states for RODE (21). The parameters in solving (17) are presented in Table VII 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 $W(\cdot,\omega) : [0,2] \to (−4,4) \times (−4,4)$, i.e., $\mathcal{W} = \{ W(\cdot,\omega) : [0,2] \to (−4,4) \times (−4,4) \mid \omega \in \Omega \}$, with probability of at least 0.98, i.e., $P(\{ \omega \in \Omega \mid W(\cdot,\omega) : [0,2] \to (−4,4) \times (−4,4) \} \geq 0.98$. Thus, the set $D$ in this case is equal to $\{ d \in \mathbb{R}^2 \mid h_1(d) \geq 0, h_2(d) \geq 0 \}$ with $h_1(d) = \sin^2 \frac{\pi}{10} - d^2$ and $h_2(d) = \sin^2 \frac{\pi}{10} - d^2$. An inner-approximation IN over the time horizon $[0,2.0]$, which is computed via solving (11), is illustrated in Fig. 8. The parameters in solving (11) are presented in Table VII and the computation time is 260.58 seconds.
Besides we use the time horizon $[0, 2]$ and the set $\mathcal{W}$ of two-dimensional Wiener paths in $C^2[0, 2]$ such that $\mathcal{W}(\cdot, \omega) : [0, 2] \to \mathbb{R}^2$. That is, the set $\mathcal{W} = \{ \mathcal{W}(\cdot, \omega) \in C^2[0, 2] \mid \omega \in \Omega \}$ includes the set of all continuous Wiener paths. Its probability measure is 1. Thus, the set $D$ in this case is $\{ d \in \mathbb{R}^2 \mid h_1(d) \geq 0, h_2(d) \geq 0 \}$ with $h_1(d) = 1 - d_1^2$ and $h_2(d) = 1 - d_2^2$. An inner-approximation $\text{IN}'$ 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 VI 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 one of the 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 [4], 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.

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.

![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 inner-approximation $\text{IN}'$ of 0.98-safe initial states. The blue curve denotes the boundary of the computed inner-approximation $\text{IN}$ of 0.98-safe initial states. The black curves denote the trajectories of RODE (21) in finite time.](image1)

![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 $\mathcal{TR}$. The green curve denotes the boundary of the computed inner-approximation $\text{IN}'$ of 0.98-safe initial states. The blue curve denotes the boundary of the computed inner-approximation $\text{IN}$ of the 0.98-safe initial states. The black curves denote the trajectories of RODE (21) in finite time.](image2)

![Fig. 10. 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 $\mathcal{TR}$. The green curve denotes the boundary of the computed inner-approximation $\text{IN}'$ of the 0.98-safe initial states. The blue curve denotes the boundary of the computed inner-approximation $\text{IN}$ of the 0.98-safe initial states. The black curves denote the trajectories of RODE (21) in finite time.](image3)
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 and that the semi-definite programs and 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, 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


