Safety Verification of Stochastic Systems: A Repetitive Scenario Approach*

Ali Salamati and Majid Zamani

***Abstract*— In this paper, we develop a *data-driven* approach for the safety verification of stochastic systems with unknown dynamics. First, we use a notion of barrier certificates in order to cast the safety verification as a robust convex program (RCP). Solving this optimization program is difficult because the model of the stochastic system, which is unknown, appears in one of the constraints. Therefore, we construct a scenario convex program (SCP) by collecting a number of samples from trajectories of the system. Then, we develop a repetition-based scenario framework to provide an out-of-sample performance guarantee for the constructed SCP. In particular, we iteratively solve an SCP for a given number of samples, and then check its feasibility using a certain number of new samples after substituting the optimal decision variables from solving the SCP. We continue the iterations until a desired violation error is achieved. Eventually, a safety condition is checked on top of the feasibility problem. If the safety condition is fulfilled, then we can provide a lower bound on the probability of safety satisfaction for the original stochastic system by leveraging the optimal solution of the successful iteration. We illustrate the effectiveness of the proposed results through a two-tank system case study, where the safety objective is to ensure that the water levels in both tanks are within some safe zones.**

I. Introduction

Safety is one of the most important requirements for designing and manufacturing complex life-critical systems. Consider a self-driving car which is not equipped with certain safety functionalities. It can cause fatal accidents, severe injuries, or serious damages to the environment. Other life-critical applications include power grids, traffic networks, and integrated medical devices, where a minor fault may have catastrophic consequences. Hence, rigorous safety analysis is required to ensure the correctness of functionalities in many safety-critical applications.

There have been many results in the past two decades on developing discretization-based or discretization-free techniques to either verify safety requirements or synthesize controllers enforcing them over complex dynamical systems. In abstraction-based techniques, e.g., [1]–[3], finite approximations are constructed by discretizing state and input sets. Those approximations are then utilized for verification and synthesis purposes. These abstraction-based techniques suffer from the curse of dimensionality due to discretizing state and input sets and, hence, they are not applicable to large-scale systems. On the other hand, some of the abstraction-free techniques utilized in the past decade leverage a notion of so-called *barrier certificates (BC)* [4], [5]. BCs are scalar-valued functions over state sets taking different values in different regions of the state set including safe and unsafe ones. Unfortunately, all of the above-mentioned discretization-based or discretization-free methods need a model of the system which may not be available or may be too complex to be of any use.

Verifying safety of dynamical systems using data has been investigated in the last few years, see, e.g., [6]–[10]. Barrier certificates and data collected from the systems' trajectories are combined in order to provide a formal guarantee on the safety, see, e.g., [11]–[15]. However, those results either suffer from the sample complexity in order to provide out-of-sample performance guarantees, may not provide any performance guarantee, require some stability assumptions, need a complete or partial knowledge of the model of the system, or not able to handle infinite time horizon specifications such as the safety specification in this paper.

Inspired by the results in [16], we propose here a so-called repetitive scenario approach that provides a data-driven framework to formally verify safety of stochastic systems with unknown models, while providing out-of-sample performance guarantees over the verification results. Similar to the results in [15] and [17], we leverage a notion of barrier certificates in order to cast the safety problem as a robust convex program (RCP). Since solving this optimization program is not tractable since the unknown model appears in one of the constraints, instead we propose a scenario convex program (SCP) corresponding to the original RCP by using N samples collected from trajectories of the system. To tackle the underlying sample complexity in the results in [15] and [17], here we construct a *repetitive scenario program* (RSP) with a specific number of iterations based on the original SCP. At each iteration, we feed the optimal solution of the SCP with N samples to a feasibility checker, called the feasibility oracle, with N_0 new test samples. The feasibility condition is defined in a way that the empirical error of the violations should be less than a desired threshold. There is a theoretical upper bound on the required number of iterations in order to satisfy the feasibility condition. Finally, a safety condition, which

*This work was supported in part by the H2020 ERC Starting Grant AutoCPS (Grant Agreement No. 804639) and the NSF under Grant CNS-2145184.

Ali Salamati is with the Computer Science Department, Ludwig-Maximilians-Universität München, Germany; email: ali.salamati@lmu.de.

Majid Zamani is with the Computer Science Department, University of Colorado Boulder, CO 80309, USA. M. Zamani is also with the Computer Science Department, LMU Munich, Germany; email: majid.zamani@colorado.edu.

is derived based on Lipschitz constants of the constraints of RCP, is checked on top of the feasibility condition. If both conditions are satisfied, then the optimal solution of the RSP is formally related to the original safety verification problem. As a result, for a fixed a-priori confidence, the unknown stochastic system is safe with a quantified probability lower bound computed using feasible solutions of the successful iteration.

The proposed approach here enables the users to select the required number of samples (i.e. N) by trading it off with the expected value of the required number of iterations: smaller amounts of N requires larger amounts of iterations and vice versa. Fortunately, these iterations are natively parallelizable which facilitates applications of our approach to large-scale systems. Finally, we apply our method to a two-tank system in order to verify whether the water levels in both tanks never reach a critical region within a specific time horizon. This case study readily shows that the computational cost of our approach is much smaller (roughly two orders of magnitude) than the one in [15], [17] in terms of sample complexity and computation time.

II. Problem Statement and Preliminaries

A. Notation

The set of positive and non-negative integers, real numbers, non-negative and positive real numbers are denoted by $\mathbb{N} := \{1, 2, 3, \ldots\}$, $\mathbb{N}_0 := \{0, 1, 2, \ldots\}$, $\mathbb{R}$, $\mathbb{R}_0^+$, and $\mathbb{R}^+$, respectively. We denote the indicator function by $\mathbb{1}_{\mathscr{A}}(X) : X \to \{0, 1\}$, where $\mathbb{1}_{\mathscr{A}}(x)$ is 1 if and only if $x \in \mathscr{A}$, and 0 otherwise. Notation $\mathbf{1}_m$ is used to indicate a column vector of ones in $\mathbb{R}^m$. We denote by $\|x\|$ the Euclidean norm of $x \in \mathbb{R}^n$. We also denote the induced norm of matrix $A \in \mathbb{R}^{m\times n}$ by $\|A\| := \sup_{x\neq 0} \|Ax\|/\|x\|$. Given N vectors $x_i \in \mathbb{R}^{n_i}$, $n_i \in \mathbb{N}$, and $i \in \{1, \ldots, N\}$, we use $[x_1; \ldots; x_N]$ and $[x_1, \ldots, x_N]$ to denote the corresponding column and row vectors, respectively, with dimension $\sum_i n_i$. Considering a random variable z, Var(z) denotes its variance. The largest integer no larger than x is denoted by $\lfloor x \rfloor$. We use the notation $S \models_H \Psi$ to denote that system S satisfies a property Ψ within a time horizon H. We also use $\models$ to show that a solution is feasible for an optimization problem.

The sample space of random variables is denoted by Ω. The Borel σ-algebra on a set X is denoted by $\mathfrak{B}(X)$. The measurable space on X is denoted by $(X, \mathfrak{B}(X))$. We have two probability spaces in this work. The first one is represented by $(X, \mathfrak{B}(X), \mathbb{P})$ which is the probability space defined over the state set X with $\mathbb{P}$ as a probability measure. The second one, $(V_w, \mathfrak{B}(V_w), \mathbb{P}_w)$, defines the probability space over V_w for the random variable w affecting the system as the process noise with $\mathbb{P}_w$ as its probability measure. With a slight abuse of notation, we use the same notation for $\mathbb{P}$ and $\mathbb{P}_w$ when the product measures are needed in the formulations. We define a so-called beta-Bionomial distribution as $f_{bb}(q, \alpha, \beta; i) = \binom{q}{i} B(i+\alpha, q-i+\beta)/B(\alpha, \beta)$ for $i = 0, 1, \ldots, q$, where $B(\alpha, \beta)^{-1} = \alpha \binom{\alpha+\beta-1}{\beta-1}, \forall \alpha, \beta \in \mathbb{N}$.

B. System Definition

In this paper, we deal with discrete-time stochastic systems as in the next definition.

Definition 1: Consider a discrete-time stochastic system (dt-SS), denoted by $S = (X, V_w, w, f)$, described by:

$$S : x(t+1) = f(x(t), w(t)), \quad t \in \mathbb{N}_0, \tag{1}$$

where X and V_w are Borel σ-algebras on the set $\mathbb{R}^n$ and the uncertainty space, respectively. Here, x denotes the state sequence of the system as $x := \{x(t) : \Omega \to X, t \in \mathbb{N}_0\}$, and w denotes a sequence of i.i.d. random variables over V_w as $w := \{w(t) : \Omega \to V_w, t \in \mathbb{N}_0\}$. Map $f : X \times V_w \to X$ is a measurable function characterizing the state evolution of the system. A finite trajectory of the system in (1) is represented by $x(0)x(1)\ldots x(t), t \in \mathbb{N}_0$. Throughout this paper, we assume the set X is compact.

C. Problem Statement

First, we formally define what it means for a system to satisfy a safety specification.

Definition 2: Consider a dt-SS S as in (1) and a safety specification denoted by the tuple $\Psi = (X_{in}, X_u, H)$, where $X_{in}, X_u \subset X$ and $H \in \mathbb{N}_0$. System S satisfies Ψ, denoted by $S \models_H \Psi$, if all trajectories of S started from initial set $X_{in} \subset X$ never reach unsafe set $X_u \subset X$ within the time horizon H.

Now, we present the main problem we solve in this paper.

> *Problem 1:* Consider a dt-SS S as in Definition 1, where f and $\mathbb{P}_w$ are *unknown*, and a safety specification Ψ as in Definition 2. With a confidence of at least $(1-\beta) \in [0, 1]$, provide a lower bound $(1-\Delta) \in [0, 1]$ on the probability with which S satisfies Ψ, i.e., $\mathbb{P}_w\big(S \models_H \Psi\big) \geq 1 - \Delta$, using data collected from trajectories of S.

The overview of our approach for solving Problem 1 is depicted in Fig. 1, which connects the related optimizations and results throughout the paper. First, a stochastic safety problem is reformulated as a scenario convex program (SCP) by collecting N samples from the state set, and $\hat{N}$ samples from the realization of the noise. The constructed scenario program is solved, and the obtained optimal solution is sent to a feasibility checker called a feasibility oracle. In this oracle, the feasibility of the SCP is assessed for N_0 new test samples by checking the constraints after substituting the optimal decision variables from the previous step. The violation of constraints is measured through an empirical mean over the violated constraints. These two steps, namely solving the SCP for collected samples and feasibility oracle, are executed for a specific number of iterations, until the violation error is less than a desired threshold. Finally, a safety condition is checked on top of the feasibility oracle. If the safety condition is satisfied, with an a-priori fixed confidence, one can conclude that the original stochastic system with unknown dynamic is safe with a probability lower bound computed using the optimal solution coming from the successful iteration.

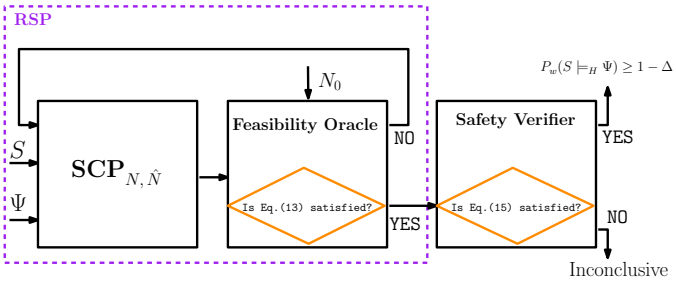

Fig. 1. An overview of our repetition-based scenario approach. The block on the left solves a scenario program SCP_{N} using $N\hat{N}$ samples collected from the system at each iteration. The resulted optimizer of this scenario program is fed into a feasibility oracle, which assesses the feasibility of the computed optimizer for N_0 new test samples. Finally, the block on the right checks a condition whose satisfaction ensures Ψ is satisfied with a probability lower-bound computed using the optimal solution of the successful iteration.

D. Safety Verification of Stochastic Systems

Here, we explain a notion of barrier certificates and its application in the safety verification of stochastic systems. Let us first formally define a barrier certificate.

Definition 3: Consider a dt-SS S as in Definition 1 and a safety specification Ψ as in Definition 2. A non-negative function $\mathrm{B}: X \to \mathbb{R}_0^+$ is called a barrier certificate (BC) for S if there exist constants $\lambda > 1$, and $c \in \mathbb{R}$ such that

$$\mathrm{B}(x) \leq 1, \qquad \forall x \in X_{in}, \tag{2}$$

$$\mathrm{B}(x) \geq \lambda, \qquad \forall x \in X_u, \tag{3}$$

$$\mathbb{E}\Big[\mathrm{B}(f(x,w)) \mid x\Big] \leq \mathrm{B}(x) + c, \qquad \forall x \in X, \tag{4}$$

where $X_{in} \subset X$ and $X_u \subset X$ are initial and unsafe sets, respectively, corresponding to Ψ (cf. Definition 2).

Next theorem, borrowed from [5], provides a lower bound on the probability of safety satisfaction for a dt-SS.

Theorem 1: Consider a dt-SS S and safety specification Ψ as in Definitions 1-2, respectively. Suppose there exists a barrier certificate B satisfying conditions (2)-(4). Then, one has

$$\mathbb{P}_w\big(S \models_H \Psi\big) \geq 1 - \frac{1 + \max\{0, c\}\ H}{\lambda}, \tag{5}$$

where $H \in \mathbb{N}_0$ is the finite time horizon associated with Ψ. Note that if $c \leq 0$ in (4), then H can be chosen arbitrarily large without affecting the lower bound in (5).

In this work, we fix the structure of barrier certificates as $B(b,x) = \sum_{j=1}^{r} b_j p_j(x)$ with some user-defined (possibly nonlinear) basis functions $p_j(x)$ and unknown coefficients $b = [b_1; \cdots; b_r] \in \mathbb{R}^r$. For the sake of simplicity of the presentation, we consider polynomial-type barrier certificates with degree $m \in \mathbb{N}_0$, where basis functions $p_j(x)$ are monomials over x. However, other basis functions such as exponential or trigonometric ones can also be handled by the proposed approach here.

III. Data-driven Safety Verification of Stochastic Systems

A. Scenario-Based Formulations for Safety Verification

According to [15], [17], a barrier-based safety verification as in Theorem 1 together with Definition 3 can be reformulated as a robust convex program (RCP):

$$\mathrm{RCP}: \begin{cases} \min\limits_{d} \quad K \\ \text{s.t.} \quad \max\big(g_z(x,d)\big) \leq 0, z \in \{1,\ldots,4\}, \forall x \in X, \\ \qquad \lambda > 1, \quad d = [K; \lambda; c; b], \end{cases} \tag{6}$$

where

$$\begin{aligned} g_1(x,d) &= -\mathrm{B}(b,x) - K, \\ g_2(x,d) &= \mathrm{B}(b,x)\mathbb{1}_{X_{in}}(x) - 1 - K, \\ g_3(x,d) &= -\mathrm{B}(b,x)\mathbb{1}_{X_u}(x) + \lambda - K, \\ g_4(x,d) &= \mathbb{E}\Big[\mathrm{B}(b, f(x,w)) \mid x\Big] - \mathrm{B}(b,x) - c - K. \end{aligned} \tag{7}$$

In general, finding an optimal solution for the RCP in (6) is difficult (or even impossible) because the map f and the probability measure $\mathbb{P}_w$ are both unknown. Furthermore, there are infinitely many constraints in the RCP since $x \in X$, where X is a continuous set. To address the issue of unknown $\mathbb{P}_w$ and the expectation term in g_4 in (7), we replace the expectation term with its empirical mean approximation by collecting $\hat{N}$ i.i.d. samples w_j, $j \in \{1,\ldots,\hat{N}\}$, from $\mathbb{P}_w$ and construct a new RCP denoted by $\mathrm{RCP}_{\hat{N}}$ as follows:

$$\mathrm{RCP}_{\hat{N}}: \begin{cases} \min\limits_{d} \quad K \\ \text{s.t.} \quad \max\big(g_z(x,d), \bar{g}_4(x,w_j,d)\big) \leq 0, z \in \{1,\ldots,3\}, \\ \qquad j \in \{1,\ldots,\hat{N}\}, \forall x \in X, \lambda > 1, d = [K; \lambda; c; b], \end{cases} \tag{8}$$

where

$$\bar{g}_4(x,w_j,d) = \frac{1}{\hat{N}} \sum_{j=1}^{\hat{N}} \mathrm{B}(b, f(x,w_j)) - \mathrm{B}(b,x) - c - K + e. \tag{9}$$

Notice that the expectation term in g_4 in (7) is approximated by the empirical mean in (9). This approximation introduces an error which is introduced by e in (9). Next theorem, borrowed from [17, Theorem 3.4], shows that the optimal solution of the $\mathrm{RCP}_{\hat{N}}$ is a feasible solution for the RCP in (6) with a certain confidence.

Theorem 2: Let d_s^* be a feasible solution of the $\mathrm{RCP}_{\hat{N}}$ for some $e > 0$, and assume $\mathrm{Var}\big(\mathrm{B}(b, f(x,w)\big) \leq \hat{M}$, $\forall x \in X$ with a given positive $\hat{M}$. Then, for any $\beta_s \in (0,1)$, one has $\mathbb{P}(d_s^* \models \mathrm{RCP}) \geq 1 - \beta_s$, if the number of samples in the empirical mean satisfies $\hat{N} \geq \frac{\hat{M}}{e^2 \beta_s}$.

Now, one can assign a probability distribution over the state set and collect N i.i.d. samples to solve $\mathrm{RCP}_{\hat{N}}$ in (8). The data-set is denoted by:

$$\begin{aligned} \mathcal{D}_{N,\hat{N}} := \big\{ (x_i, w_j, f(x_i,w_j)) \subset X \times V_w \times X \mid \\ i \in \{1,\ldots,N\}, j \in \{1,\ldots,\hat{N}\} \big\}. \end{aligned} \tag{10}$$

By substituting these samples in $\text{RCP}_{\hat{N}}$ in (8) results in the following SCP denoted by $\text{SCP}_{N,\hat{N}}$:

$$\text{SCP}_{N,\hat{N}}: \begin{cases} \min\limits_{d} \quad K \\ \text{s.t.} \ \max\left(g_z(x_i,d), \bar{g}_4(x_i,w_j,d)\right) \leq 0, \\ \quad \lambda > 1, z \in \{1,2,3\}, i \in \{1,\ldots,N\}, \\ \quad j \in \{1,\ldots,\hat{N}\}, d = [K;\lambda;c;b]. \end{cases} \tag{11}$$

B. Repetitive Scenario Program

Inspired by the the idea of repetitive scenario design in [16], we aim at constructing an RSP for the stochastic safety problem. The main idea is to solve an $\text{SCP}_{N,\hat{N}}$ in (11) for several iterations. At each iteration, the obtained optimal values denoted by $d^*_{N,\hat{N}}$ are used to construct a feasibility problem denoted by $\text{SCP}_{N_0,\hat{N}}$ using N_0 new test samples. The violation criteria for the constraints using the k^{th} sampled data, where $k \in \{1,\ldots,N_0\}$, in the constructed feasibility problem at each iteration can be quantified as:

$$v_{N,\hat{N}}(k) = \begin{cases} 1 \quad \min\left(-g_z(x_k,d^*_{N,\hat{N}}), -\bar{g}_4(x_k,w_j,d^*_{N,\hat{N}})\right) \leq 0, \\ \quad z \in \{1,2,3\}, j \in \{1,\ldots,\hat{N}\}, \\ 0 \quad \text{otherwise.} \end{cases} \tag{12}$$

Now, we define the concept of *successful iteration*.

Definition 4: The overall violation error for N_0 test samples can be computed by applying an empirical mean over all violated constraints at each iteration and can be upper bounded by a given desired value:

$$\frac{\sum_{k=1}^{N_0} v_{N,\hat{N}}(k)}{N_0} \leq \epsilon'. \tag{13}$$

We call the first iteration at which the above condition is satisfied the successful iteration.

Now, we introduce Algorithm 1 to systematically construct an RSP to solve the original safety problem (Problem 1) in Algorithm 2. The optimal solution of the RSP resulted from Algorithm 1 is denoted by d^*.

Algorithm 1 Repetitive Scenario Program (RSP Algorithm)

Require: Number of samples (N, $\hat{N}$, and N_0) and the desired violation error ϵ'

1: Collect $\hat{N}$ samples $w_j, j \in [1,\ldots,\hat{N}]$ from $\mathbb{P}_w$
2: Collect N samples $x_i, i \in [1,\ldots,N]$ from the state set
3: Solve the $\text{SCP}_{N,\hat{N}}$ in (11) using the collected data in Step 1 and Step 2, and obtain the optimizer $d^*_{N,\hat{N}}$
4: Feasibility Oracle: Construct the feasibility problem $\text{SCP}_{N_0,\hat{N}}$ using N_0 new samples by feeding the optimal values from Step 3 to the scenario program in (11)
5: Compute $\frac{\sum_{k=1}^{N_0} v_{N,\hat{N}}(k)}{N_0}$ for $v_{N,\hat{N}}(k)$ as in (12)
6: If (13) is satisfied, then $d^* = d^*_{N,\hat{N}}$, otherwise go to Step 2.

Remark 1: According to [16, Theorem 3], Algorithm 1 terminates within $(1-H_{1,\epsilon'.}(N))^{-1}$ iterations with probability one, where $H_{1,\epsilon'}(N) = 1-\sum_{i=0}^{\lfloor \epsilon' N_0 \rfloor} f_{bb}(N_0,|d|,N+1-|d|;i)$, f_{bb} is the beta-Binomial distribution, and $|d|$ is the number of decision variables in (11). Furthermore, for the large values of N_0, the expected number of iterations in order to satisfy (13), and accordingly termination of the algorithm, is approximated by

$$\frac{1}{1-\beta_{\epsilon'}(N)}, \tag{14}$$

where $\beta_{\epsilon'}(N) = 1 - \sum_{i=|d|}^{N} \binom{N}{i} \epsilon'^i (1-\epsilon')^{N-i}$. For the sake of simple presentation, we use this approximation in the rest of the paper.

In the next section, we relate the optimal solution of an RSP to that of RCP in (6) and finally to the safety of stochastic systems.

IV. Safety Verification of Stochastic Systems

Here, we provide a probabilistic connection between the optimal value of a repetitive scenario optimization program RSP as in Algorithm 1 and the safety of stochastic systems with unknown dynamics in Definition 1. The next theorem provides the relation between the solution of a repetitive scenario program and the original safety problem.

Theorem 3: Consider a stochastic system S as in (1), where f and $\mathbb{P}_w$ are *unknown*, and a safety specification Ψ as in Definition 2. Assume all constraints in (7) are Lipschitz continuous[a] with respect to x and with a Lipschitz constant L_x. Let $\epsilon, \epsilon' \in [0,1], \epsilon' \leq \epsilon$. Choose $\hat{N}$ as in Theorem 2 based on a given confidence $1-\beta_s, \beta_s \in (0,1)$. Suppose that for a given N and N_0, there is a successful iteration (cf. Definition 4) for RSP in Algorithm 1, for which the optimal solution is $d^* = [K^*;\lambda^*;c^*;b^*]$. If

$$K^* + \text{L}_\text{x}\, \epsilon^{\frac{1}{n}} \leq 0, \tag{15}$$

then

$$\mathbb{P}_w(\text{S} \models_H \Psi) \geq 1 - \frac{1+c^*H}{\lambda^*}, \tag{16}$$

with a confidence of at least $1 - \bar{\beta}_{\epsilon,\epsilon'}(N,N_0) - \beta_s$, where

$$\bar{\beta}_{\epsilon,\epsilon'}(N,N_0) = 1 - \sum_{i=\lfloor |d| + \epsilon' N_0 - 1 \rfloor + 1}^{N+N_0} \binom{N+N_0}{i} \epsilon^i (1-\epsilon)^{N+N_0-i},$$

and $|d|$ is the number of decision variables in (11).

[a] We only need to consider Lipschitz continuity of g_2 and g_3 inside X_{in} and X_u, respectively.

Proof: From the robust convex program $\text{RCP}_{\hat{N}}$ in (8), one can construct a chance constraint program as:

$$\text{CCP}_\epsilon: \begin{cases} \min\limits_{d} \quad K \\ \text{s.t.} \ \mathbb{P}\left(\max\left(g_z(x,d), \bar{g}_4(x,w_j,d)\right) \leq 0\right) \geq 1-\epsilon, \\ \quad j \in \{1,\ldots,\hat{N}\}, z \in \{1,\ldots,3\}, \\ \quad \lambda > 1, d = [K;\lambda;c;b], \end{cases} \tag{17}$$

for some $\epsilon > 0$, where $g_z(x,d),\ z \in \{1,\ldots,3\}$, and $\bar{g}_4$ are defined in (7) and (9), respectively. Using Theorem 3 in [16]

and for a given N and N_0, one obtains

$$\mathbb{P}\big(d^* \models \text{CCP}_\epsilon\big) \geq 1 - \bar{\beta}_{\epsilon,\epsilon'}(N, N_0), \tag{18}$$

for some $\epsilon' \leq \epsilon$, where $d^* = [K^*; \lambda^*; c^*; b^*]$ is the optimal solution of the RSP in Algorithm 1. Now, we construct a relaxed version of $\text{RCP}_{\hat{N}}$ in (8) as follows:

$$\text{RCP}_{h(\epsilon)}: \begin{cases} \min\limits_{d} \quad K \\ \text{s.t.} \ \max\big(g_z(x,d), \bar{g}_4(x, w_j, d)\big) \leq h(\epsilon), \\ \quad j \in \{1, \ldots, \hat{N}\}, z \in \{1, \ldots, 3\}, \forall x \in X, \\ \quad \lambda > 1, \ d = [K; \lambda; c; b], \end{cases} \tag{19}$$

where $h(\epsilon)$ is a uniform level-set bound as defined in [18, Definition 3.1]. According to [16], N_0 can be selected such that $\bar{\beta}_{\epsilon,\epsilon'}(N, N_0) \leq \beta_\epsilon(N)$. As a result, one can use Lemma 3.2 in [18] and conclude from (18) that $\mathbb{P}\big(d^* \models \text{RCP}_{h(\epsilon)}\big) \geq 1 - \bar{\beta}_{\epsilon,\epsilon'}(N, N_0)$, which readily results in $\mathbb{P}(K^*_{\text{RCP}_{h(\epsilon)}} \leq K^*) \geq 1 - \bar{\beta}_{\epsilon,\epsilon'}(N, N_0)$. The last inequality is true mainly because $K^*_{\text{RCP}_{h(\epsilon)}}$ is the optimal value of $\text{RCP}_{h(\epsilon)}$ in (19), whereas K^* is just the optimization value for a feasible solution (i.e. d^*). Using Lemma 3.4 in [18], we obtain $K^* \leq K^*_{\text{RCP}_{\hat{N}}} \leq K^*_{\text{RCP}_{h(\epsilon)}} + \mathcal{L}_{sp} h(\epsilon)$, where $K^*_{\text{RCP}_{\hat{N}}}$ is the optimal value of $\text{RCP}_{\hat{N}}$ in (8), and $\mathcal{L}_{sp}$ is the Slater constant defined in [18, Assumption 3.3]. Therefore, one can deduce $\mathbb{P}\Big(K^* \leq K^*_{\text{RCP}_{\hat{N}}} \leq K^* + \mathcal{L}_{sp} h(\epsilon)\Big) \geq 1 - \bar{\beta}_{\epsilon,\epsilon'}(N, N_0)$. Since the optimization problem in (8) is a min-max problem, $\mathcal{L}_{sp}$ can be chosen as 1 according to Remark 3.5 in [18]. Uniform level-set bound $h(\epsilon)$ can be computed as $\text{L}_\text{x} \sqrt[n]{\epsilon}$ as stated in [18, Remark 3.8], where L_x is the Lipschitz constant of constraints. Therefore, we have $\mathbb{P}\Big(K^* \leq K^*_{\text{RCP}_{\hat{N}}} \leq K^* + \text{L}_\text{x} \ \epsilon^{\frac{1}{n}}\Big) \geq 1 - \bar{\beta}_{\epsilon,\epsilon'}(N, N_0)$. Let us denote the optimal solution of the RCP in (8) by $d^*_{\text{RCP}_{\hat{N}}}$. We get $\mathbb{P}\big(d^*_{\text{RCP}_{\hat{N}}} \models \text{RCP}\big) \geq 1 - \beta_s$ for a specific $\hat{N}$ according to Theorem 2. This inequality implies $\mathbb{P}\big(K^*_{\text{RCP}} \leq K^*_{\text{RCP}_{\hat{N}}}\big) \geq 1 - \beta_s$, where K^*_{RCP} is the optimal value of the RCP in (6). By defining events $\mathcal{A} := \{K^* \leq K^*_{\text{RCP}_{\hat{N}}} \leq K^* + \text{L}_\text{x} \ \epsilon^{\frac{1}{n}}\}$ and $\mathcal{B} := \{K^*_{\text{RCP}} \leq K^*_{\text{RCP}_{\hat{N}}}\}$, where $\mathbb{P}(\mathcal{A}) \geq 1 - \bar{\beta}_{\epsilon,\epsilon'}(N, N_0)$ and $\mathbb{P}(\mathcal{B}) \geq 1 - \beta_s$, it is easy to see that $(\mathcal{A} \cap \mathcal{B}) \subseteq (K^*_{\text{RCP}} \leq K^* + \text{L}_\text{x} \ \epsilon^{\frac{1}{n}})$. By the assumption of the theorem, we have $K^* + \text{L}_\text{x} \ \epsilon^{\frac{1}{n}} \leq 0$. Hence, one obtains $\mathbb{P}(K^* + \text{L}_\text{x} \ \epsilon^{\frac{1}{n}} \leq 0) \geq \mathbb{P}(\mathcal{A} \cap \mathcal{B}) \geq 1 - \mathbb{P}(\mathcal{A}^c) - \mathbb{P}(\mathcal{B}^c) \geq 1 - \bar{\beta}_{\epsilon,\epsilon'}(N, N_0) - \beta_s$. This concludes the proof since $K^*_{\text{RCP}} \leq 0$ implies that the feasible solution of RCP in (6) satisfies the barrier conditions in Theorem 1 with a confidence of at least $1 - \bar{\beta}_{\epsilon,\epsilon'}(N, N_0) - \beta_s$. ■

Remark 2: According to [16, Remark 2], for a given number of samples N, the desired level of confidence β, number of decision variables $|d|$, and $\delta = \epsilon - \epsilon'$, a lower bound for N_0 can be computed as

$$N_0 \geq \frac{\frac{\epsilon}{\delta} \ \ln \beta^{-1} + |d| - 1 - N(\frac{\delta}{2} + \epsilon')}{\delta}, \tag{20}$$

to ensure $\bar{\beta}_{\epsilon,\epsilon'}(N, N_0) \leq \beta$.

Based on the results in Theorem 3, we provide Algorithm 2 to systematically verify the safety of a stochastic system with an unknown dynamic. The coefficients of the barrier certificate satisfying conditions (2)-(4) are obtained in Step 4 of Algorithm 2.

Remark 3: Remark that there is a trade off (pareto curve) between the expected number of iterations in (14) and the number of samples N (cf. Figure 2 in the case study). Hence, the user can decide how to pick N based on the number of expected iterations within which Algorithm 1 terminates.

Algorithm 2 Data-driven safety verification

Require: Parameters $\beta \in (0,1)$, $\beta_s \in (0,1)$, $\epsilon, \epsilon' \in [0,1]$, $\epsilon' \leq \epsilon$, $\text{L}_\text{x} \in \mathbb{R}^+$, and the degree of the barrier certificate

1: Choose the number of samples N according to Remark 3
2: Compute the number of test samples N_0 according to (20)
3: Compute $\hat{N}$ according to Theorem 2
4: Call Algorithm 1 to get $d^* = [K^*; \lambda^*; c^*; b^*]$
5: Safety Verifier: If $K^* + \text{L}_\text{x} \epsilon^{\frac{1}{n}} \leq 0$, then $\mathbb{P}_w(S \models_H \Psi) \geq 1 - \frac{1 + c^* H}{\lambda^*}$ with a confidence of at least $1 - \bar{\beta}_{\epsilon,\epsilon'}(N, N_0) - \beta_s$.

V. Case Study

Consider a two-tank system modelled by the following discrete-time stochastic system:

$$\begin{aligned} \text{h}_1(t+1) &= (1 - \tau_s \frac{\alpha_1}{A_1}) \ \text{h}_1(t) + \tau_s \frac{q_i(t)}{A_1} + w_1(t) \\ \text{h}_2(t+1) &= \tau_s \frac{\alpha_1}{A_2} \text{h}_1(t) + (1 - \tau_s \frac{\alpha_2}{A_2}) \text{h}_2(t) + \tau_s \frac{q_o(t)}{A_2} + w_2(t), \end{aligned} \tag{21}$$

where $\text{h}_1(t)$ and $\text{h}_2(t)$ are heights of two tanks. Terms $w_1(t)$ and $w_2(t)$ are additive zero-mean Gaussian noises with standard deviations of 0.01, which model the environmental uncertainties. Parameters α_i and A_i, $i \in \{1, 2\}$, are valve coefficients and the area of tank i. Variables $q_i(t)$ and $q_0(t)$ are inflow rate entering the first tank and outflow rate exiting the second tank at time t, respectively. The model for this two-tank system is adapted from [19] discretized by $\tau_s = 0.1$ seconds. We consider state and input matrices as $A_\tau = [1 - \tau_s, 0; \tau_s, 1 - \tau_s]$ and $b_\tau = [\tau_s; \tau_s]$, respectively, in the situation in which input and output valves are fully open, and two constant-rate feeding and retaining pumps ensure constant flows of $q_i(t)$ and $q_o(t)$ with values of $4.5m^3/s$ and $3m^3/s$, respectively. Let us consider $X_{in} = [1.75m, 2.25m]^2$, $X_u = [9m, 10m]^2$, and $X = [1m, 10m]^2$ as the initial, unsafe and the overall state sets, respectively. We assume the model in (21) and the distribution of the noise are unknown. The main goal is to verify that the heights of both tanks stay away from the unsafe region within the time horizon $H = 5$ with an a-priori confidence 99%. Let us consider a barrier certificate with degree $k = 2$ in the polynomial form as $[\text{h}_1; \text{h}_2; 1]^T \text{P} [\text{h}_1; \text{h}_2; 1] = b_0 \text{h}_1^2 + b_1 \text{h}_2^2 + b_2 \text{h}_1 \text{h}_2 + b_3 \text{h}_1 + b_4 \text{h}_2 + b_5$, where P is a matrix containing the coefficients of the barrier certificate. By enforcing $\|\text{P}\| \leq 0.2$ and since $\|x\| \leq \sqrt{2} \times 10$, the Lipschitz constant is $\text{L}_x = 11.03$ [15, Lemma 1].

We use Algorithm 2 to apply our proposed approach to this example. We select $\epsilon = 0.65 \times 10^{-4}$, $\epsilon' = 0.7\epsilon = 0.45 \times 10^{-4}$, $\beta_s = 0.001$, and $\beta = 0.009$. Then, one needs to select

the number of samples N. This can be done by considering the trade-off between N and the number of the required iterations according to Remark 3 (cf. Fig. 2). For example, for 10^6, 10^5, and 5×10^4 number of samples, the expected required iterations are 1, 59, and 8283, respectively. Here, we select $N = 70000$ for which the expected number of iterations is 636. The number of test samples is computed as $N_0 = 1017100$ using (20). The value of $\hat{N}$ is computed as 400 according to Theorem 2 by considering the approximation error in (9) as $e = 0.05$ and enforcing $\hat{M} = 0.001$. The value of $\hat{M}$ was checked a posteriori using enough number of data. This provides a confidence of $1 - \beta_s$, where $\beta_s = 0.001$. In Step 4, we run Algorithm 1. The algorithm terminates in only 5 iterations, which is much less than the expected one (i.e. 636). This shows that our proposed approach is even more scalable in practice, and the theoretical upper bound is too conservative to cover the worst-case scenarios. The obtained optimal value of the successful iteration is $K^* = -0.1119$. According to Step 5 in Algorithm 2, since $K^* + \mathrm{L}_{\mathrm{x}} \epsilon^{\frac{1}{n}} = -0.0230 \leq 0$, one can conclude that the water levels remain in the safe zone with a probability lower bounded of 0.90, and this statement is true with a confidence of at least 0.9985. Remark that the number of samples, which is 70000 here, is much less than 1337297, based on the results in [15] and [17], while our approach provides an even *better confidence* (i.e. 0.9985 in comparison to 0.99). The numerical experiments were conducted using CVX [20] under MATLAB. The total computation time here was 22 seconds, which is much less than 2 hours needed to run an SCP, as in [15] and [17], for 1337297 number of samples. Furthermore, Step 4 in Algorithm 2, the most expensive part of the algorithm, is natively parallelizable. Hence, our approach can be applied to large-scale systems.

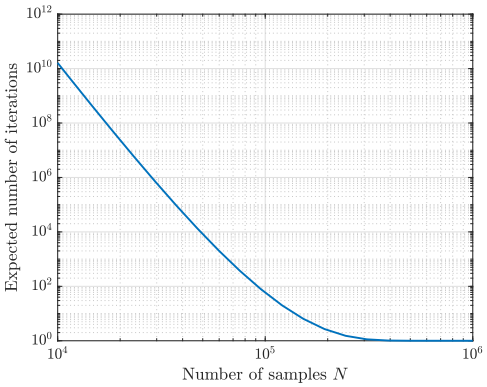

Fig. 2. Pareto diagram of expected number of iterations versus N.

VI. Conclusion

In this paper, we developed a data-driven verification approach based on the idea of repetitive scenario design. First, we constructed a repetitive scenario program based on an RCP characterizing the main safety problem as an optimization one. At each iteration of the proposed repetitive scheme, we first solve an SCP, then feed the optimizer to a feasibility oracle to check the feasibility of the SCP for a certain number of new samples before checking a rigorous safety condition on top of the feasibility one. Once both conditions (feasibility and safety) are satisfied, a lower bound can be computed for the probability of the safety of the stochastic system with unknown model by leveraging the optimal solutions of the successful iteration. Finally, the effectiveness of our approach in comparison with the existing results in [15], [17] was illustrated via a two-tank system.

References

[1] P. Tabuada, *Verification and Control of Hybrid Systems: A Symbolic Approach*. Springer, 2009.

[2] C. Belta, B. Yordanov, and E. A. Gol, *Formal methods for discrete-time dynamical systems*. Springer, 2017, vol. 15.

[3] M. Zamani, P. M. Esfahani, R. Majumdar, A. Abate, and J. Lygeros, "Symbolic control of stochastic systems via approximately bisimilar finite abstractions," *IEEE Transactions on Automatic Control*, vol. 59, no. 12, pp. 3135–3150, 2014.

[4] S. Prajna and A. Jadbabaie, "Safety verification of hybrid systems using barrier certificates," in *International Workshop on Hybrid Systems: Computation and Control*. Springer, 2004, pp. 477–492.

[5] P. Jagtap, S. Soudjani, and M. Zamani, "Formal synthesis of stochastic systems via control barrier certificates," *IEEE Transactions on Automatic Control*, 2020.

[6] S. Sadraddini and C. Belta, "Formal guarantees in data-driven model identification and control synthesis," in *Proceedings of the 21st International Conference on Hybrid Systems: Computation and Control (part of CPS Week)*, 2018, pp. 147–156.

[7] V. B. Wijesuriya and A. Abate, "Bayes-adaptive planning for data-efficient verification of uncertain Markov decision processes," in *International Conference on Quantitative Evaluation of Systems*. Springer, 2019, pp. 91–108.

[8] Z. Wang and R. M. Jungers, "Scenario-based set invariance verification for black-box nonlinear systems," *IEEE Control Systems Letters*, vol. 5, no. 1, pp. 193–198, 2020.

[9] L. Lindemann, N. Matni, and G. J. Pappas, "STL robustness risk over discrete-time stochastic processes," *arXiv preprint arXiv:2104.01503*, 2021.

[10] G. Agha and K. Palmskog, "A survey of statistical model checking," *ACM Transactions on Modeling and Computer Simulation (TOMACS)*, vol. 28, no. 1, pp. 1–39, 2018.

[11] S. Han, U. Topcu, and G. J. Pappas, "A sublinear algorithm for barrier-certificate-based data-driven model validation of dynamical systems," in *54th IEEE conference on decision and control (CDC)*, 2015, pp. 2049–2054.

[12] A. Robey, H. Hu, L. Lindemann, H. Zhang, D. V. Dimarogonas, S. Tu, and N. Matni, "Learning control barrier functions from expert demonstrations," in *2020 59th IEEE Conference on Decision and Control (CDC)*. IEEE, 2020, pp. 3717–3724.

[13] P. Jagtap, G. J. Pappas, and M. Zamani, "Control barrier functions for unknown nonlinear systems using Gaussian processes," in *2020 59th IEEE Conference on Decision and Control (CDC)*. IEEE, 2020, pp. 3699–3704.

[14] L. Lindemann, H. Hu, A. Robey, H. Zhang, D. V. Dimarogonas, S. Tu, and N. Matni, "Learning hybrid control barrier functions from data," *arXiv:2011.04112*, 2020.

[15] A. Salamati, A. Lavaei, S. Soudjani, and M. Zamani, "Data-driven safety verification of stochastic systems," *7th IFAC Conference on Analysis and Design of Hybrid Systems*, 2021.

[16] G. C. Calafiore, "Repetitive scenario design," *IEEE Transactions on Automatic Control*, vol. 62, no. 3, pp. 1125–1137, 2016.

[17] A. Salamati, A. Lavaei, S. Soudjani, and M. Zamani, "Data-driven verification and synthesis of stochastic systems through barrier certificates," *Arxiv*, 2021.

[18] P. M. Esfahani, T. Sutter, and J. Lygeros, "Performance bounds for the scenario approach and an extension to a class of non-convex programs," *IEEE Transactions on Automatic Control*, vol. 60, no. 1, pp. 46–58, 2014.

[19] J. A. Ramos and P. L. Dos Santos, "Mathematical modeling, system identification, and controller design of a two tank system," in *46th IEEE Conference on Decision and Control*. IEEE, 2007, pp. 2838–2843.

[20] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1," http://cvxr.com/cvx, 2014.