Preprints of the 21st IFAC World Congress (Virtual)
Berlin, Germany, July 12-17, 2020

Synthesis of Stochastic Systems with Partial Information via Control Barrier Functions [⋆]

Niloofar Jahanshahi [†, ∗] **Pushpak Jagtap** [†, ∗∗] **Majid Zamani** [∗∗∗,∗]

[∗] *Ludwig Maximilian University of Munich, Germany,*
(*e-mail: niloofar.jahanshahi@lmu.de*).
[∗∗] *Technical University of Munich, Germany,*
(*e-mail: pushpak.jagtap@tum.de*)
[∗∗∗] *University of Colorado Boulder, USA,*
(*e-mail: majid.zamani@colorado.edu*)

Abstract: Synthesis of controllers for stochastic control systems ensuring safety constraints has gained considerable attention in the last few years. In this paper, we consider the problem of synthesizing controllers for partially observed stochastic control systems to ensure finite-time safety. Given an estimator with a probabilistic guarantee on the accuracy of the estimations, we provide an approach to compute a controller providing a lower bound on the probability that the trajectories of the stochastic control system remain safe over a finite time-horizon. To obtain such controllers, we utilize a notion of control barrier functions. We also provide an approach to compute a probability bound on estimator accuracy by using a notion of so-called stochastic simulation function. The proposed result is illustrated on a case study.

Keywords: Control Barrier Functions, Safety Synthesis, Stochastic Control Systems, Partial Information, Output Feedback Control.

1. INTRODUCTION

Safety is an important design objective in many control systems such as automobiles, aviation, energy, and medicine. Failure in ensuring safety could result in loss of life or damage to the system and environment. For this reason research on formal synthesis of controllers enforcing safety specifications has gained considerable attentions in the last few years. The discrete abstraction based techniques are quite popular for formal synthesis of safety controllers (Tabuada, 2009; Belta et al., 2017; Girard et al., 2015, and references therin). However, these techniques suffer from the curse of dimensionality since the computational complexity increases exponentially with the dimension of the state-space.

On the other hand, the discretization-free approaches, using barrier functions, has shown potential for solving verification or synthesis of deterministic and stochastic systems against safety specifications (see (Prajna et al., 2007; Ames et al., 2014; Ames et al., 2019; Jagtap et al., 2018, 2019, 2020; Anand et al., 2019; Huang et al., 2017)). However, all the aforementioned results assume the availability of the full state information which is not the case in many real-world applications. Assuming a prior knowledge of the control barrier functions, (Clark, 2019) provides synthesis of controllers for stochastic control systems with incomplete information. However, in order to provide infinite time horizon guarantees, this result requires that the control barrier functions exhibit supermartingale property which presupposes stochastic stability and vanishing noise at the equilibrium point of the system.

In this paper, we consider the problem of formal synthesis of stochastic control systems with partial state information ensuring safety specification over finite-time horizon *without* requiring any assumption on the stability of the stochastic system. In order to achieve this, we do not require the supermartingale property on control barrier functions.

Our main contribution is to provide a systematic approach for computing a lower bound on the probability that the stochastic control system with partial information satisfies safety specifications over a finite-time horizon. Given an appropriate estimator with a probabilistic guarantee on the closeness of the estimator's and system's trajectories, we provide sufficient conditions for control barrier functions under which one can provide the lower bound on the probability of satisfying safety specifications over a finite time-horizon. Then, we provide sufficient conditions for computing control barrier functions and corresponding controllers. We also provide an approach to compute probability bound on the estimator accuracy for a class of stochastic control systems by utilizing a notion of so-called stochastic simulation function (Julius et al. (2006); Julius and Pappas (2008)).

[⋆] This work was supported in part by the H2020 ERC Starting Grant AutoCPS, the German Research Foundation (DFG) through the grants ZA 873/1-1 and the Research Training Group 2428, and the TUM International Graduate School of Science and Engineering (IGSSE).

[†] The authors contributed equally to this work.

The rest of the paper is organized as follow: In Section 2, we define stochastic control systems with incomplete information and the required assumptions. Then, we formally define the problem statement. The notion of control barrier functions and their computation are explained in Section 3. Section 4 provides a systematic approach on computing estimator accuracies by utilizing a notion of so-called stochastic simulation functions. The case study and conclusion are given in Sections 5 and 6, respectively.

2. STOCHASTIC CONTROL SYSTEMS

2.1 Notations

We denote the set of real, positive real, and non-negative real numbers by $\mathbb{R}$, $\mathbb{R}^+$, and $\mathbb{R}_0^+$, respectively. We use $\mathbb{R}^n$ to denote the n-dimensional Euclidean space and $\mathbb{R}^{n\times r}$ to denote the space of real matrices with n rows and r columns. Given a matrix $A \in \mathbb{R}^{n\times n}$, $\mathrm{Tr}(A)$ represents trace of A which is the sum of all diagonal elements of A. We use $\lambda_{\min}(A)$ to represent the minimum eigenvalue of the symmetric matrix A. The zero matrix in $\mathbb{R}^{n\times m}$ is denoted by $0_{n\times m}$. Given a vector $x \in \mathbb{R}^n$, we denote by $\|x\|$ the Euclidean norm of x. The diagonal set $\Delta \subset \mathbb{R}^{2n}$ is defined as $\Delta = \{(x,x), x \in \mathbb{R}^n\}$. A continuous function $\alpha : \mathbb{R}_0^+ \to \mathbb{R}_0^+$ belongs to class $\mathcal{K}$ if it is strictly increasing and $\alpha(0) = 0$; it belongs to class $\mathcal{K}_\infty$ if $\alpha \in \mathcal{K}$ and $\alpha(r) \to \infty$ as $r \to \infty$.

2.2 Problem Formulation

Let the triplet $(\Omega, \mathcal{F}, \mathbb{P})$ denote a probability space with a sample space Ω, filtration $\mathcal{F}$, and the probability measure $\mathbb{P}$. The filtration $\mathbb{F} = (\mathcal{F}_s)_{s\geq 0}$ satisfies the usual conditions of right continuity and completeness (Øksendal, 2000). Let $(W_s)_{s\geq 0}$ and $(V_s)_{s\geq 0}$ be $\bar{r}$- and r-dimensional $\mathbb{F}$-Brownian motions, respectively, which are independent of each other.

Definition 2.1. A stochastic control system with output is a tuple $\Sigma = (\mathbb{R}^n, \mathbb{R}^m, \mathcal{U}, f, g, \mathbb{R}^p, h, \sigma)$, where

- $\mathbb{R}^n$ is the state space;
- $\mathbb{R}^m$ is the input space;
- $\mathcal{U}$ is a subset of all $\mathbb{F}$-progressively measurable processes with values in $\mathbb{R}^m$, (see (Karatzsas and Shreve, 1991));
- $f : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ satisfies the following Lipschitz assumption: there exist constants $L_x, L_u \in \mathbb{R}^+$ such that $\|f(x,u) - f(x',u')\| \leq L_x\|x - x'\| + L_u\|u - u'\|$, $\forall x, x' \in \mathbb{R}^n$ and $\forall u, u' \in \mathbb{R}^m$;
- $g : \mathbb{R}^n \to \mathbb{R}^{n\times r}$ satisfies the following Lipschitz assumption: there exists a constant $L_g \in \mathbb{R}_0^+$ such that $\|g(x) - g(x')\| \leq L_g\|x - x'\|$, $\forall x, x' \in \mathbb{R}^n$;
- $\mathbb{R}^p$ is the output space;
- $h : \mathbb{R}^n \to \mathbb{R}^p$ satisfies the following Lipschitz assumption: there exists a constant $L_h \in \mathbb{R}^+$ such that $\|h(x) - h(x')\| \leq L_h\|x - x'\|$, $\forall x, x' \in \mathbb{R}^n$;
- $\sigma : \mathbb{R}^n \to \mathbb{R}^{p\times\bar{r}}$ satisfies the following Lipschitz assumption: there exists a constant $L_\sigma \in \mathbb{R}_0^+$ such that $\|\sigma(x) - \sigma(x')\| \leq L_\sigma\|x - x'\|$, $\forall x, x' \in \mathbb{R}^n$.

A stochastic process $\xi : \Omega \times \mathbb{R}_0^+ \to \mathbb{R}^n$ is said to be a *solution process* of Σ if there exists $\upsilon \in \mathcal{U}$ satisfying the stochastic differential equations (SDE)

$$\Sigma : \begin{cases} \mathrm{d}\,\xi &= f(\xi,\upsilon)\,\mathrm{d}\,t + g(\xi)\,\mathrm{d}\,V_t, \\ \mathrm{d}\,y &= h(\xi)\,\mathrm{d}\,t + \sigma(\xi)\,\mathrm{d}\,W_t, \end{cases} \tag{2.1}$$

where $y(t)$ taking values in $\mathbb{R}^p$ denotes the output of Σ and represents the noisy partial information at each time $t \in \mathbb{R}_0^+$ $\mathbb{P}$-almost surely ($\mathbb{P}$-a.s.). A partially observed system is considered since in most practical cases, the physical state of the system can only be partially determined by direct observation. Solution process of Σ exists and is unique due to the assumptions on f and g (Øksendal, 2000). We assume that the pair $(\frac{\partial f}{\partial x}(x,u), h(x))$ is uniformly detectable (Clark, 2019, Definition 6). Throughout the paper, we use the notation $\xi_{a\upsilon}(t)$ to denote the value of the solution process at time $t \in \mathbb{R}_0^+$ under the input signal υ starting from the initial state $\xi_{a\upsilon}(0) = a$ $\mathbb{P}$-a.s., in which a is a random variable that is measurable in $\mathcal{F}_0$.

For the later use, we provide the definition of the infinitesimal generator (denoted by operator $\mathcal{D}$) for a stochastic control system Σ using Ito's differentiation (Øksendal, 2000). Let $B : \mathbb{R}^n \to \mathbb{R}$ be a twice differentiable function. The infinitesimal generator of B associated with the system Σ for all $x \in \mathbb{R}^n$ and for all $u \in U$ is given by

$$\mathcal{D}B(x,u) = \frac{\partial B}{\partial x}(x)f(x,u) + \frac{1}{2}\mathrm{Tr}\big(g^T(x)\frac{\partial^2 B}{\partial x^2}(x)g(x)\big). \tag{2.2}$$

In order to provide the results in this paper, we raise the following assumption on the existence of the estimator that estimates the state of the partial information system (2.1) with a probabilistic guarantee on the estimation accuracy.

Assumption 2.2. The states of the partially observed stochastic control system Σ in (2.1) can be estimated by a proper estimator $\hat{\Sigma}$ represented in the form of stochastic differential equation with the estimated state trajectory $\hat{\xi}(t)$ which is described by:

$$\hat{\Sigma} : \mathrm{d}\,\hat{\xi} = f(\hat{\xi},\upsilon)\,\mathrm{d}\,t + K\big(\mathrm{d}\,y - h(\hat{\xi})\,\mathrm{d}\,t\big), \tag{2.3}$$

where $K \in \mathbb{R}^{n\times p}$ is the estimator gain. Moreover, the probabilistic bound on the accuracy of the estimator is given as (Reif et al., 2000):

$$\forall\delta \in (0,1] \;\; \exists\epsilon > 0 \;\; \text{such that}$$
$$\mathbb{P}\Big(\sup_{t\geq 0}\|\xi_{a\upsilon}(t) - \hat{\xi}_{\hat{a}\upsilon}(t)\| \leq \epsilon\Big) \geq 1 - \delta. \tag{2.4}$$

To find the relation between ϵ and δ, one can use the notion of so-called stochastic simulation functions introduced in (Julius and Pappas, 2009). The construction of stochastic simulation functions and the probability bound for the case of linear stochastic control systems is provided in Section 4.

Now, we formally define the main synthesis problem in this work.

Problem 2.3. Given a partially observed stochastic control system Σ in (2.1), given an estimator (2.3) satisfying (2.4), sets $X_0 \subset \mathbb{R}^n$, $X_1 \subset \mathbb{R}^n$, compute a controller (if existing) and a real value $\vartheta \in (0,1)$ such that the probability of the solution process of Σ starting from X_0 and not reaching X_1 over the finite time horizon $T \in \mathbb{R}^+$ is lower bounded by ϑ (*i.e.,* $\mathbb{P}\{\forall t \in [0,T),\; \xi_{a\upsilon}(t) \notin X_1\} \geq \vartheta$, $\forall a \in X_0$.

Finding a solution to Problem 2.3 (if existing) is difficult in general. In this paper, we provide a sound method in solving this problem. To synthesize a controller, we utilize the notion of control barrier functions introduced in the next section.

3. CONTROL BARRIER FUNCTIONS

In this section, we provide sufficient conditions using so-called control barrier functions under which we can provide the lower bound on the probability that the trajectories of system Σ start from any initial state in set $X_0 \subset \mathbb{R}^n$ and do not reach unsafe set $X_1 \subset \mathbb{R}^n$. In order to provide this result, we first define an ϵ-inflated version of X_1 as $X_1^\epsilon := \{\hat{x} \mid \exists x \in X_1, \|\hat{x} - x\| \leq \epsilon\}$. Now we provide an intermediate result providing an upper bound on the reachability probability for the trajectory of the estimator $\hat{\Sigma}$ in (2.3).

Theorem 3.1. Consider a partially observed stochastic control system Σ in (2.1), an estimator $\hat{\Sigma}$ with the accuracy ϵ as in (2.4), and sets $X_0, X_1^\epsilon \subset \mathbb{R}^n$. Suppose there exists a twice differentiable function $B : \mathbb{R}^n \to \mathbb{R}_0^+$, constants $c \geq 0$ and $\gamma \in [0, 1]$ such that

$$B(\hat{x}) \leq \gamma \quad \forall \hat{x} \in X_0, \tag{3.1}$$

$$B(\hat{x}) \geq 1 \quad \forall \hat{x} \in X_1^\epsilon, \tag{3.2}$$

$$\begin{aligned} &\inf_{u\in U} \frac{\partial B}{\partial \hat{x}}(\hat{x}) f(\hat{x}, u) + L_h \epsilon \|\frac{\partial B}{\partial \hat{x}}(\hat{x}) K\| \\ &+ \frac{1}{2}\mathrm{Tr}\Big(\sigma^T(\hat{x}) K^T \frac{\partial^2 B}{\partial \hat{x}^2}(\hat{x}) K \sigma(\hat{x})\Big) \leq c \quad \forall \hat{x} \in \mathbb{R}^n, \end{aligned} \tag{3.3}$$

where $L_h \in \mathbb{R}_0^+$ is the Lipschitz constant for the function h. Then, the probability that the solution process $\hat{\xi}$ of the estimator $\hat{\Sigma}$ starting from an initial state $\hat{a} \in X_0$ and reaching region X_1^ϵ within time horizon $[0, T) \subset \mathbb{R}_0^+$ is upper bounded by $\gamma + cT$.

Proof. Consider the infinitesimal generator associated with the estimator $\hat{\Sigma}$ as

$$\begin{aligned} \mathcal{D}B(\hat{x}, u) =& \frac{\partial B}{\partial \hat{x}}(\hat{x})\Big(f(\hat{x}, u) + K\big(h(x) - h(\hat{x})\big)\Big) \\ &+ \frac{1}{2}\mathrm{Tr}\Big(\sigma^T(\hat{x}) K^T \frac{\partial^2 B}{\partial \hat{x}^2}(\hat{x}) K \sigma(\hat{x})\Big). \end{aligned}$$

If $\|x - \hat{x}\| \leq \epsilon$, then one gets

$$\begin{aligned} \frac{\partial B}{\partial \hat{x}}(\hat{x}) K\big(h(x) - h(\hat{x})\big) &\leq \|\frac{\partial B}{\partial \hat{x}}(\hat{x}) K\| \|h(x) - h(\hat{x})\| \\ &\leq \|\frac{\partial B}{\partial \hat{x}}(\hat{x}) K\| L_h \epsilon. \end{aligned}$$

Hence, if (3.3) holds, then

$$\begin{aligned} &\inf_{u\in U} \frac{\partial B}{\partial \hat{x}}(\hat{x})\Big(f(\hat{x}, u) + K\big(h(x) - h(\hat{x})\big)\Big) \\ &\qquad + \frac{1}{2}\mathrm{Tr}\Big(\sigma^T(\hat{x}) K^T \frac{\partial^2 B}{\partial \hat{x}^2}(\hat{x}) K \sigma(\hat{x})\Big) \\ &\leq \inf_{u\in U} \frac{\partial B}{\partial \hat{x}}(\hat{x}) f(\hat{x}, u) + L_h \epsilon \|\frac{\partial B}{\partial \hat{x}}(\hat{x}) K\| \\ &\qquad + \frac{1}{2}\mathrm{Tr}\Big(\sigma^T(\hat{x}) K^T \frac{\partial^2 B}{\partial \hat{x}^2}(\hat{x}) K \sigma(\hat{x})\Big) \leq c. \end{aligned}$$

Thus, one has $\inf_{u\in U} \mathcal{D}B(\hat{x}, u) \leq c$. Now by utilizing (Kushner, 1967, Theorem 1), (3.1), and the fact that $X_1^\epsilon \subseteq \{\hat{x} \in \mathbb{R}^n \mid B(\hat{x}) \geq 1\}$, we have $\mathbb{P}\{\hat{\xi}_{\hat{a}\upsilon}(t) \in X_1^\epsilon \text{ for some } 0 \leq t < T \mid \hat{\xi}_{\hat{a}\upsilon}(0) = \hat{a}\} \leq \mathbb{P}\{\sup_{0\leq t<T} B(\hat{\xi}_{\hat{a}\upsilon}(t)) \geq 1 \mid \hat{\xi}_{\hat{a}\upsilon}(0) = \hat{a}\} \leq B(\hat{a}) + cT \leq \gamma + cT$ which concludes the proof. □

The function B in Theorem 3.1 satisfying (3.1) - (3.3) is usually referred to as the control barrier function.

Remark 3.2. The above theorem gives controller as the infimum over u of the left-hand side of inequality (3.3).

The result of Theorem 3.1 guarantees that the following inequality holds:

$$\mathbb{P}\Big\{\exists t \in [0, T),\ \hat{\xi}_{\hat{a}\upsilon}(t) \in X_1^\epsilon\Big\} \leq \gamma + Tc, \tag{3.4}$$

In the next theorem, we provide the upper bound on the reachability property over the trajectory of the original system Σ by utilizing the bound obtained in Theorem 3.1 and the estimator accuracy.

Theorem 3.3. Consider a partially observed stochastic control system Σ in (2.1), an estimator $\hat{\Sigma}$ with the accuracy ϵ as in (2.4), the results in Theorem 3.1, and sets $X_0, X_1, X_1^\epsilon \subset \mathbb{R}^n$. Then for any $a \in X_0$

$$\mathbb{P}\Big\{\exists t \in [0, T),\ \xi_{a\upsilon}(t) \in X_1\Big\} \leq \gamma + Tc + \delta. \tag{3.5}$$

Proof. The proof is inspired by the proof of Corollary 3.5 in (Lavaei et al., 2017). Given $a, \hat{a} \in X_0$, let us define the events $A_1 := \{\exists t \in [0, T),\ \xi_{a\upsilon}(t) \in X_1\}$ and $A_2 := \{\exists t \in [0, T),\ \hat{\xi}_{\hat{a}\upsilon}(t) \in X_1^\epsilon\}$. Then, we have

$$\mathbb{P}\{A_1\} = \mathbb{P}\{A_1 \cap A_2\} + \mathbb{P}\{A_1 \cap \bar{A}_2\} \leq \mathbb{P}\{A_2\} + \mathbb{P}\{A_1 \cap \bar{A}_2\},$$

where $\bar{A}_2$ is the complement of A_2. Notice that the term $\mathbb{P}\{A_1 \cap \bar{A}_2\}$ is bounded by δ according to (2.4) and the definition X_1^ϵ. This concludes the proof. □

Corollary 3.4. Given the results in Theorem 3.3, the probability that the trajectories of Σ start from any $a \in X_0$ and stay in $\mathbb{R}^n \setminus X_1$ is lower bounded by

$$\mathbb{P}\Big\{\forall t \in [0, T),\ \xi_{a\upsilon}(t) \notin X_1\Big\} \geq 1 - (\gamma + Tc + \delta). \tag{3.6}$$

3.1 Computation of Control Barrier Functions

Proving the existence of a control barrier function and finding one are in general hard problems. However, one can search for parametric barrier functions of the form $B(q, \hat{x}) = \sum_{i=1}^{\mathsf{r}} q_i b_i(\hat{x})$ with some user-defined (possibly nonlinear) basis functions $b_i(\hat{x})$ and unknown coefficients $q_i \in \mathbb{R}$, $i \in \{1, 2, \ldots, \mathsf{r}\}$, and the parametric state feedback controller of the similar form. The following lemma provides a set of sufficient conditions for the existence of such a parametric control barrier function required in Theorem 3.1, which can be solved as an optimization problem.

Lemma 3.5. Consider compact sets X_0, X_1^ϵ, $X \subset \mathbb{R}^n$ as given in Theorem 3.1. Suppose there exists a parametric function $B(q, \hat{x})$ and parametric functions $\psi_{u_i}(d_{u_i}, \hat{x})$ corresponding to the i^{th} input in $u = (u_1, u_2, \ldots, u_m) \in U \subset \mathbb{R}^m$ with vectors of parameters q and d_{u_i} of appropriate sizes, respectively, constants $c \geq 0$ and $\gamma \in [0, 1]$ that satisfy

$$B(q, \hat{x}) \geq 0 \quad \forall \hat{x} \in X, \tag{3.7}$$

$$B(q, \hat{x}) \leq \gamma \quad \forall \hat{x} \in X_0, \tag{3.8}$$

$$B(q, \hat{x}) \geq 1 \quad \forall \hat{x} \in X_1^\epsilon, \tag{3.9}$$

$$\frac{\partial B}{\partial \hat{x}}(q,\hat{x})f(\hat{x},u)+L_h\epsilon\|\frac{\partial B}{\partial \hat{x}}(q,\hat{x})K\|+\sum_{i=1}^{m}(u_i-\psi_{u_i}(d_{u_i},\hat{x}))$$
$$+\frac{1}{2}\mathrm{Tr}\Big(\sigma^T(\hat{x})K^T\frac{\partial^2 B}{\partial \hat{x}^2}(q,\hat{x})K\sigma(\hat{x})\Big)\leq c \quad \forall \hat{x}\in X, \forall u\in U. \tag{3.10}$$

Then $B(q,\hat{x})$ satisfies conditions in Theorem 3.1 and $u_i = \psi_{u_i}(d_{u_i},\hat{x})$ is the corresponding control policy.

Proof. The first three conditions implies (3.1) and (3.2) along with non-negativeness of the function B. Now, if we choose control input $u_i = \psi_{u_i}(d_{u_i},\hat{x})$, condition (3.10) implies (3.3) in Theorem 3.1 which concludes the proof. □

In order to search for the parameters q and d_{u_i} in Lemma 3.5 satisfying (3.7)-(3.10), one can use existing nonlinear optimization solvers such as (Gurobi Optimization, 2019). Note that, the methods may run into local optima, however, one can utilize multi-start techniques (Marti, 2003) to obtain global optima. For the final rigorous verification step, one can use tools such as dReal (Gao et al., 2013) or RSolver (Ratschan, 2006) to formally verify that the computed functions indeed satisfy the required conditions. In order to compute δ in (3.6), we utilize the notion of stochastic simulation function which is introduced in the next section.

4. STOCHASTIC SIMULATION FUNCTION

In this section, we define a notion of stochastic simulation functions similar to the one defined by (Julius and Pappas, 2009) which can be used to quantify the distance (a.k.a. error) between a system's state and its estimation as in inequality (2.4).

We first define the augmented process $\begin{bmatrix}\xi & \hat{\xi}\end{bmatrix}^T$, where ξ and $\hat{\xi}$ are the solution processes of Σ and $\hat{\Sigma}$, respectively. The corresponding augmented stochastic control system is given as

$$\mathrm{d}\begin{bmatrix}\xi\\ \hat{\xi}\end{bmatrix}=\left(\begin{bmatrix}f(\xi,u)\\ f(\hat{\xi},u)\end{bmatrix}+\begin{bmatrix}0_{n\times p} & 0_{n\times p}\\ K & -K\end{bmatrix}\begin{bmatrix}h(\xi)\\ h(\hat{\xi})\end{bmatrix}\right)\mathrm{d}\,t$$
$$+\begin{bmatrix}g(\xi) & 0_{n\times\bar{r}}\\ 0_{n\times r} & K\sigma(\xi)\end{bmatrix}\begin{bmatrix}\mathrm{d}\,V_t\\ \mathrm{d}\,W_t\end{bmatrix}. \tag{4.1}$$

Next, we define a notion of stochastic solution functions which can be used to obtain the probability bound in (2.4).

Definition 4.1. A continuous function $\phi:\mathbb{R}^n\times\mathbb{R}^n\to\mathbb{R}_0^+$ that is twice differentiable on $\mathbb{R}^n\times\mathbb{R}^n\setminus\Delta$ is a *stochastic simulation function* from $\hat{\Sigma}$ to Σ if

(i) for all $(x,\hat{x})\in\mathbb{R}^n\times\mathbb{R}^n$, $\phi(x,\hat{x})\geq\alpha(\|x-\hat{x}\|)$, where α is a $\mathcal{K}_\infty$-function;
(ii) for all $u\in\mathbb{R}^m$, $(x,\hat{x})\in\mathbb{R}^n\times\mathbb{R}^n$ there exists a constant $\bar{c}\geq 0$ and $\kappa\geq 0$ such that $\mathcal{D}\phi(x,\hat{x},u)\leq-\kappa\phi(x,\hat{x})+\bar{c}$, where the operator $\mathcal{D}$ is acting on the augmented dynamics in (4.1).

The next result provides the probability bound on the estimation accuracy by using the stochastic simulation function.

Theorem 4.2. Consider stochastic systems Σ and $\hat{\Sigma}$ with dynamics as in (2.1) and (2.3), respectively, and a stochastic simulation function $\phi:\mathbb{R}^n\times\mathbb{R}^n\to\mathbb{R}_0^+$ from $\hat{\Sigma}$ to Σ. Then for any $\upsilon\in\mathcal{U}$, any $\epsilon\in\mathbb{R}^+$, and any $a,\hat{a}\in\mathbb{R}^n$ the following holds:

$$\mathbb{P}\Big(\sup_{0\leq t\leq T}\|\xi_{a\upsilon}(t)-\hat{\xi}_{a\upsilon}(t)\|\geq\epsilon\mid a,\hat{a}\Big)$$
$$\leq 1-\big(1-\frac{\phi(a,\hat{a})}{\alpha(\epsilon)}\big)e^{-\bar{c}T/\alpha(\epsilon)},\quad \text{if } \alpha(\epsilon)\geq\frac{\bar{c}}{\kappa}, \tag{4.2}$$

$$\mathbb{P}\Big(\sup_{0\leq t\leq T}\|\xi_{a\upsilon}(t)-\hat{\xi}_{\hat{a}\upsilon}(t)\|\geq\epsilon\mid a,\hat{a}\Big)$$
$$\leq\frac{\phi(a,\hat{a})+(e^{\kappa T}-1)(\bar{c}/\kappa)}{\alpha(\epsilon)e^{\kappa T}},\quad \text{if } \alpha(\epsilon)\leq\frac{\bar{c}}{\kappa}, \tag{4.3}$$

where $T>0$ is the time horizon.

Proof. Since ϕ is a stochastic simulation function from $\hat{\Sigma}$ to Σ, one obtains the following chain of inequality

$$\mathbb{P}\Big(\sup_{0\leq t\leq T}\|\xi_{a\upsilon}(t)-\hat{\xi}_{\hat{a}\upsilon}(t)\|\geq\epsilon\mid a,\hat{a}\Big)$$
$$=\mathbb{P}\Big(\sup_{0\leq t\leq T}\alpha(\|\xi_{a\upsilon}(t)-\hat{\xi}_{\hat{a}\upsilon}(t))\|\geq\alpha(\epsilon)\mid a,\hat{a}\Big)$$
$$\leq\mathbb{P}\Big(\sup_{0\leq t\leq T}\phi(\xi_{a\upsilon}(t),\hat{\xi}_{\hat{a}\upsilon}(t))\geq\alpha(\epsilon)\mid a,\hat{a}\Big)$$
$$\leq\begin{cases}1-\big(1-\dfrac{\phi(a,\hat{a})}{\alpha(\epsilon)}\big)e^{-\bar{c}T/\alpha(\epsilon)}, & \text{if } \alpha(\epsilon)\geq\dfrac{\bar{c}}{\kappa},\\[2ex] \dfrac{\phi(a,\hat{a})+(e^{\kappa T}-1)(\bar{c}/\kappa)}{\alpha(\epsilon)e^{\kappa T}}, & \text{if } \alpha(\epsilon)\leq\dfrac{\bar{c}}{\kappa}.\end{cases}$$

The equality holds due to the fact that α is a $\mathcal{K}_\infty$ function. The second inequality holds based on condition (i) of Definition 4.1, and the last inequality follows from the result in (Kushner, 1965, Theorem 1). □

Next, we provide sufficient conditions under which we can construct a stochastic simulation function for linear stochastic control systems. Consider the following linear stochastic control system

$$\Sigma:\begin{cases}\mathrm{d}\,\xi &= (A\xi+B\upsilon)\,\mathrm{d}\,t+g(\xi)\,\mathrm{d}\,V_t,\\ \mathrm{d}\,y &= C\xi\,\mathrm{d}\,t+\sigma(\xi)\,\mathrm{d}\,W_t,\end{cases} \tag{4.4}$$

and the corresponding linear estimator as

$$\hat{\Sigma}:\mathrm{d}\,\hat{\xi}=(A\hat{\xi}+B\upsilon)\,\mathrm{d}\,t+K(\mathrm{d}\,y-C\hat{\xi}\,\mathrm{d}\,t). \tag{4.5}$$

Next, we impose the following assumption in order to provide the main result of this section.

Assumption 4.3. Consider the linear system Σ in (4.4). We assume that there exist a positive definite matrix P, gain K, and a constant $\kappa\in\mathbb{R}_0^+$ such that the following matrix inequality holds

$$(A^T-C^TK^T)P+P(A-KC)<-\kappa P. \tag{4.6}$$

Note that if pair (A,C) is observable, then there always exists such choices of P and K.

From now on we assume that we are interested in studying behaviours of Σ over compact set $X\subset\mathbb{R}^n$. In the following lemma, we provide sufficient conditions under which one can have a quadratic stochastic simulation function from $\hat{\Sigma}$ to Σ.

Lemma 4.4. Consider a linear stochastic control systems Σ and estimator $\hat{\Sigma}$ as in (4.4) and (4.5), respectively.

Assume Σ satisfies Assumption 4.3 and for all $x \in X$ there exists $\bar{c} \geq 0$ such that

$$\operatorname{Tr}\left([g(x) \ -K\sigma(x)]^T \, P \, [g(x) \ -K\sigma(x)] \right) \leq \bar{c}. \tag{4.7}$$

Then

$$\phi(x,\hat{x}) = (x-\hat{x})^T P(x-\hat{x}), \tag{4.8}$$

is a stochastic simulation function from $\hat{\Sigma}$ to Σ.

Proof. By following (2.2), the infinitesimal generator acting on the function ϕ is as follows:

$$\begin{aligned}\mathcal{D}\phi(x,\hat{x}) =& (x-\hat{x})^T[(A^T - C^T K^T)P \\ &+ P(A-KC)](x-\hat{x}) \\ &+ \operatorname{Tr}\left([g(x) \ -K\sigma(x)]^T \, P \, [g(x) \ -K\sigma(x)] \right) \\ \leq& -\kappa\phi(x,\hat{x}) + \bar{c}.\end{aligned}$$

The inequality follows from (4.6) and (4.7) which implies condition (ii) of Definition 4.1 being satisfied. Condition (i) of Definition 4.1 is satisfied by choosing

$$\alpha(s) = \frac{1}{2}\lambda_{\min}(P)s^2. \qquad \square$$

5. CASE STUDY

In this section, we consider a DC motor to demonstrate the effectiveness of our results. Consider the dynamics of a DC motor given using stochastic differential equation as follows:

$$\Sigma : \begin{cases} \mathrm{d}\begin{bmatrix}\xi_1 \\ \xi_2\end{bmatrix} = \left(\overbrace{\begin{bmatrix} -\dfrac{R}{L} & -\dfrac{K_{dc}}{L} \\ -\dfrac{K_{dc}}{J} & -\dfrac{b}{J}\end{bmatrix}}^{A} \begin{bmatrix}\xi_1 \\ \xi_2\end{bmatrix} + \begin{bmatrix}\dfrac{1}{L} \\ 0\end{bmatrix} \upsilon \right) \mathrm{d}\,t \\ \qquad + \begin{bmatrix} 0.05 & 0 \\ 0 & 0.05\end{bmatrix} \mathrm{d}\,V_t, \\ \mathrm{d}\,y = \underbrace{[0 \ 1]}_{C} \begin{bmatrix}\xi_1 \\ \xi_2\end{bmatrix} \mathrm{d}\,t + 0.01\,\mathrm{d}\,W_t, \end{cases} \tag{5.1}$$

where $\xi_1, \xi_2, \upsilon, R, L$ and J are the armature current, the rotational speed of the shaft, the voltage source applied to the motor's armature, the resistance, the inductance, and the moment of inertia of the rotor, respectively. V_t and W_t denote the standard Brownian motions. Constant K_{dc} represents both the motor torque constant and the back emf constant. The values of the parameters are $J = 0.01$, $b = 0.1$, $K_{dc} = 0.01$, $R = 1$, and $L = 0.5$, which are adopted from (Jahanshahi et al., 2016). From matrices A and C, one can readily see that the system is observable. We consider the state set $X = [-0.1 \ 0.1] \times [-0.5 \ 0.5]$, and regions of interest $X_0 = [-0.01 \ 0.01] \times [-0.2 \ 0.2]$, $X_1 = [-0.1 \ -0.05] \times [-0.5 \ -0.3] \cup [0.05 \ 0.1] \times [0.3 \ 0.5]$. The aim is to compute a controller with a potentially tight upper bound on the probability of the states starting from the initial set X_0 reaching the unsafe set X_1 within time horizon $T = 10$, as in (3.5).

We compute matrices

$$K = \begin{bmatrix}0.0069 \\ 0.0027\end{bmatrix}, P = \begin{bmatrix}0.0554 & 0.0053 \\ 0.0053 & 0.3209\end{bmatrix},$$

and $\kappa = 0.1$ satisfying (4.6) by converting it to an LMI using Schur complement. The stochastic simulation function according to Lemma 4.4 is given as $\phi(x,\hat{x}) = (x-\hat{x})^T P(x-\hat{x})$ with $\alpha(s) = 0.02768s^2$ and $\bar{c} = 3.7693 \times 10^{-7}$. By use of the results in Theorem 4.2 we obtain $\delta = 0.1272$ by choosing $\epsilon = 0.01$. The obtained probability that is at least 87.28% is also empirically verified by computing distance between trajectories of the concrete system and the estimated system at time using 10000 realizations. Several realizations are shown in Figure 1.

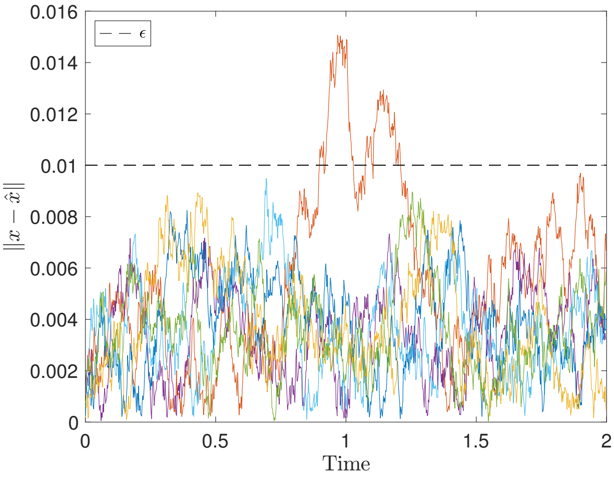

Fig. 1. A few realizations of the errors between concrete state trajectories and estimated trajectories.

A quadratic control barrier function using the approach discussed in Subsection 3.1 is obtained as follows:

$$B(\hat{x}) = 290.9438\hat{x}_1^2 + 10.98940\hat{x}_1\hat{x}_2 + 1.1977\hat{x}_2^2,$$

and the corresponding control policy as

$$\mathbf{u}(\hat{x}) = 0.2721\hat{x}_1 + 1.3607\hat{x}_2. \tag{5.2}$$

with the values $\gamma = 0.099$, $c = 1 \times 10^{-5}$, $T = 10$. All the computations are done using GUROBI and YALMIP (Löfberg, 2004). The lower bound in (3.6) is computed as:

$$\mathbb{P}\left\{\forall t \in [0,T), \xi_{av}(t) \notin X_1\right\} \geq 0.77369, \ \forall a \in X_0.$$

Figure 2 shows a few realizations of the trajectories starting from the initial region X_0 under the control policy (5.2).

6. CONCLUSIONS

We provided a framework for designing control barrier functions for partially observed stochastic control systems subjected to noisy measurements. The controllers associated with control barrier functions provide the upper bound on the probability that the system reaches an unsafe region in a finite time horizon. This upper bound is provided by utilizing the probability bound obtained for the accuracy of the estimator via the notion of stochastic simulation functions. The effectiveness of the results are demonstrated on a case study.

REFERENCES

Ames, A.D., Coogan, S., Egerstedt, M., Notomista, G., Sreenath, K., and Tabuada, P. (2019). Control barrier functions: Theory and applications. In *2019 18th*

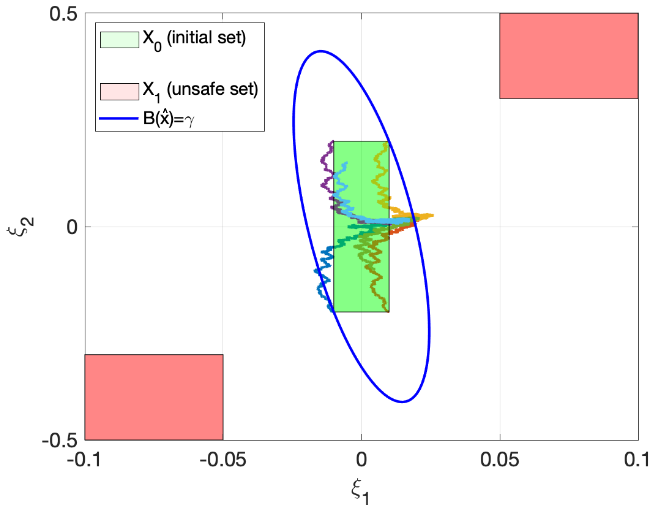

Fig. 2. A few realizations of the closed-loop trajectories using controller (5.2). The blue ellipsoid shows the γ-level set of B, defined as $\{\hat{x} \in X \mid B(\hat{x}) = \gamma\}$.

European Control Conference (ECC), 3420–3431. doi: 10.23919/ECC.2019.8796030.

Ames, A.D., Grizzle, J.W., and Tabuada, P. (2014). Control barrier function based quadratic programs with application to adaptive cruise control. In *53rd IEEE Conference on Decision and Control*, 6271–6278. IEEE.

Anand, M., Jagtap, P., and Zamani, M. (2019). Verification of switched stochastic systems via barrier certificates. In *2019 IEEE 58th Conference on Decision and Control (CDC)*, 4373–4378. IEEE.

Belta, C., Yordanov, B., and Gol, E.A. (2017). *Formal methods for discrete-time dynamical systems*, volume 89. Springer.

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

Gao, S., Kong, S., and Clarke, E.M. (2013). dReal: An SMT solver for nonlinear theories over the reals. In *International Conference on Automated Deduction*, 208–214. Springer.

Girard, A., Gössler, G., and Mouelhi, S. (2015). Safety controller synthesis for incrementally stable switched systems using multiscale symbolic models. *IEEE Transactions on Automatic Control*, 61(6), 1537–1549.

Gurobi Optimization, L. (2019). Gurobi optimizer reference manual. URL `http://www.gurobi.com`.

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

Jagtap, P., Soudjani, S., and Zamani, M. (2018). Temporal logic verification of stochastic systems using barrier certificates. In *International Symposium on Automated Technology for Verification and Analysis*, 177–193. Springer.

Jagtap, P., Soudjani, S., and Zamani, M. (2019). Formal synthesis of stochastic systems via control barrier certificates. *arXiv preprint arXiv:1905.04585*.

Jagtap, P., Swikir, A., and Zamani, M. (2020). Compositional construction of control barrier functions for interconnected control systems. In *Proceedings of the 23rd International Conference on Hybrid Systems: Computation and Control*, 1–11.

Jahanshahi, N., Meskin, N., Abdollahi, F., and Haddad, W.M. (2016). An adaptive sliding mode observer for linear systems under malicious attack. In *2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 001437–001442. IEEE.

Julius, A.A. and Pappas, G.J. (2008). Probabilistic testing for stochastic hybrid systems. In *2008 47th IEEE Conference on Decision and Control*, 4030–4035. IEEE.

Julius, A.A. and Pappas, G.J. (2009). Approximations of stochastic hybrid systems. *IEEE Transactions on Automatic Control*, 54(6), 1193–1203.

Julius, A.A., Girard, A., and Pappas, G.J. (2006). Approximate bisimulation for a class of stochastic hybrid systems. In *2006 American Control Conference*, 6–pp. IEEE.

Karatzsas, I. and Shreve, S.E. (1991). Brownian motion and stochastic calculus. *Graduate texts in Mathematics*, 113.

Kushner, H.J. (1965). On the stability of stochastic dynamical systems. *Proceedings of the National Academy of Sciences*, 53(1), 8–12.

Kushner, H. (1967). Stochastic stability and control, ser. *Mathematics in Science and Engineering. New York: Academic Press*.

Lavaei, A., Soudjani, S.E.Z., Majumdar, R., and Zamani, M. (2017). Compositional abstractions of interconnected discrete-time stochastic control systems. In *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, 3551–3556. IEEE.

Löfberg, J. (2004). Yalmip: A toolbox for modeling and optimization in matlab. In *Proceedings of the CACSD Conference*, volume 3. Taipei, Taiwan.

Marti, R. (2003). *Multi-Start Methods*, 355–368. Springer US, Boston, MA.

Øksendal, B. (2000). *Stochastic Differential Equations: An Introduction with Applications*. Springer-Verlag, Berlin.

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

Ratschan, S. (2006). Efficient solving of quantified inequality constraints over the real numbers. *ACM Transactions on Computational Logic (TOCL)*, 7(4), 723–748.

Reif, K., Gunther, S., Yaz, E., and Unbehauen, R. (2000). Stochastic stability of the continuous-time extended kalman filter. *IEE Proceedings-Control Theory and Applications*, 147(1), 45–52.

Tabuada, P. (2009). *Verification and control of hybrid systems: a symbolic approach*. Springer Science & Business Media.