Brief paper

Control barrier functions for stochastic systems☆

Andrew Clark

Department of Electrical and Computer Engineering, Worcester Polytechnic Institute, 100 Institute Road, Worcester, MA 01609, United States of America

ARTICLE INFO

ABSTRACT

Control Barrier Functions (CBFs) aim to ensure safety by constraining the control input at each time step so that the system state remains within a desired safe region. This paper presents a framework for CBFs in stochastic systems in the presence of Gaussian process and measurement noise. We first consider the case where the system state is known at each time step, and present reciprocal and zero CBF constructions that guarantee safety with probability 1. We extend our results to high relative degree systems and present both general constructions and the special case of linear dynamics and affine safety constraints. We then develop CBFs for incomplete state information environments, in which the state must be estimated using sensors that are corrupted by Gaussian noise. We prove that our proposed CBF ensures safety with probability 1 when the state estimate is within a given bound of the true state, which can be achieved using an Extended Kalman Filter when the system is linear or the process and measurement noise are sufficiently small. We propose control policies that combine these CBFs with Control Lyapunov Functions in order to jointly ensure safety and stochastic stability. Our results are validated via numerical study on a multi-agent collision avoidance scenario.

1. Introduction

Safety, defined as ensuring that the state of a control system remains within a particular region, is an essential property in applications including transportation, medicine, and energy. The need for safety has motivated extensive research into synthesizing and verifying controllers to satisfy safety requirements. Methodologies include barrier methods (Prajna, Jadbabaie, & Pappas, 2007), discrete approximations (Chutinan, 1999; Mitra, Wongpiromsarn, & Murray, 2013; Ratschan & She, 2005), and reachable set computation (Althoff, Le Guernic, & Krogh, 2011; Girard, Le Guernic, & Maler, 2006).

Recently, Control Barrier Functions (CBFs) have emerged as a promising approach to ensure safety while maintaining computational tractability (Ames, Xu, Grizzle, & Tabuada, 2016). A CBF is a function that either decays to zero (Zero CBF, or ZCBF) or diverges to infinity (Reciprocal CBF, or RCBF) as the state trajectory approaches the boundary of the safe region. Safety of the system can be guaranteed by adding a constraint to the control input, which ensures that the CBF remains finite in the case of RCBF

and positive in the case of ZCBF (Fig. 1). The CBF approach has been successfully applied to bipedal locomotion (Hsu, Xu, & Ames, 2015; Nguyen & Sreenath, 2016b), automotive control (Chen, Peng, & Grizzle, 2017; Mehra et al., 2015), and UAVs (Wu & Sreenath, 2016). Furthermore, by composing a CBF with a Control Lyapunov Function (CLF), optimization-based control policies with joint guarantees on safety and stability can be designed.

Existing CBF techniques are applicable to deterministic systems with exact observation of the system state. Many control systems, however, operate in the presence of noise in both the system dynamics and sensor measurements. A CBF framework for stochastic systems would enable computationally tractable control with probabilistic guarantees on safety by making the CBF method applicable to a broader class of systems.

In this paper, we generalize CBF-based methods for safe control to stochastic systems. We consider complete information systems, in which the exact system state is known, as well as incomplete information systems in which only noisy measurements of the state are available. For both cases, we formulate stochastic versions ZCBF and RCBF, and show that a linear constraint on the control at each time step results in provable safety guarantees. We make the following contributions:

- In the complete information case, we formulate ZCBFs and RCBFs and derive sufficient conditions for the system to satisfy safety with probability 1.
- In the incomplete information case, we consider a class of controllers in which the state estimate is obtained via
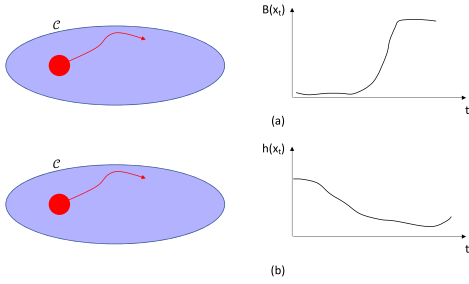
Fig. 1. Illustration of (a) Reciprocal CBF and (b) Zero CBF.

Extended Kalman Filter (EKF). We derive bounds on the probability of violating the safety constraints as a function of the estimation error of the filter.

- We derive sufficient conditions for constructing ZCBFs for high relative degree systems, and analyze the special case of linear systems with affine safety constraints and complete state information.
- We construct optimization-based controllers that integrate stochastic CLFs with CBFs to ensure safety and performance. The controllers solve quadratic programs at each time step and thus can be implemented on embedded systems.
- We evaluate our approach via numerical study on multi-agent collision avoidance. We find that the proposed ZCBF guarantees safety while still allowing the agents to reach their desired final states.

The rest of the paper is organized as follows. Section 3 presents needed background. Section 4 presents CBF constructions in the complete information case. Section 5 considers the incomplete information case. Section 6 presents control policy constructions via stochastic CBFs. Section 7 contains numerical results. Section 8 concludes the paper.

2. Related work

The CBF method for synthesizing safe controllers was proposed in Ames, Grizzle, and Tabuada (2014) and Ames et al. (2016). For a comprehensive survey of recent work on CBFs, see Ames et al. (2019). Composition of CBFs with CLFs for guaranteed safety and stability was proposed in Romdlony and Jayawardhana (2016). CBFs have been proposed for input-constrained systems (Rauscher, Kimmel, & Hirche, 2016), systems with delays (Jankovic, 2018), self-triggered systems (Yang, Belta, & Tron, 2019), and linearizable systems (Xu, 2018). Extensions to incorporate signal temporal logic constraints were developed in Lindemann and Dimarogonas (2019). A framework for *exponential CBFs* that enable safety guarantees in high relative-degree systems was proposed in Nguyen and Sreenath (2016a). High relative-degree deterministic systems were also considered in Khojasteh, Dhiman, Franceschetti, and Atanasov (2020) and Xiao and Belta (2019). While the present paper also considers high relative degree systems, we propose a different approach and, moreover, consider the problem in a stochastic setting. Learning-based methods for CBFs in systems with incomplete information due to uncertainties were presented in Cheng, Khojasteh, Ames, and Burdick (2020), Cheng, Orosz, Murray, and Burdick (2019), Fan et al. (2020) and Khojasteh et al. (2020).

The problem of verifying safety of a given system and controller has been studied extensively over the past several decades (Chutinan, 1999; Dolginova & Lynch, 1997; Ratschan & She, 2005; Tabuada, 2009; Tomlin, Pappas, & Sastry, 1998). In the verification literature, the approach that is closest to the present work is

the barrier function method (Prajna & Jadbabaie, 2004; Prajna et al., 2007). Barrier certificates provide provable guarantees that a system with given controller does not enter an unsafe region. More recently, a tighter barrier function construction that enables controller synthesis for stochastic systems was proposed in Santoyo, Dutreix, and Coogan (2019). Barrier certificate methods, however, enable safety verification of a given system, but do not provide an approach for synthesizing controllers with safety guarantees. Indeed, existing techniques for synthesizing barrier certificates using sum-of-squares optimization are inapplicable to designing control barrier functions. A discrete-time barrier certificate for ensuring satisfaction of temporal logic properties via control barrier functions was proposed in Jagtap, Soudjani, and Zamani (2020), however, this problem setting differed from our continuous-time, infinite-horizon approach. A finite-horizon sum-of-squares based CBF for continuous systems was proposed in Jahanshahi, Jagtap, and Zamani (2020).

The preliminary conference version of this paper (Clark, 2019) introduced CBFs for stochastic systems, including what this paper refers to as *reciprocal CBFs*. The present paper introduces the additional notion of *zero CBFs* for stochastic systems, as well as methodologies for computing CBFs for high relative degree systems. We also extend our results in the incomplete information case to systems where the output is nonlinear in the input.

3. Background

This section provides background on martingales and stochastic differential equations (SDEs). In what follows, we let $\cdot^+ = \max\{\cdot, 0\}$, $\cdot^- = \min\{\cdot, 0\}$, $\mathbf{E}(\cdot)$ denote expectation, and $\mathbf{tr}(\cdot)$ denote the trace. A function $\alpha : \mathbb{R} \to \mathbb{R}$ is *class-K* if it is strictly increasing and $\alpha(0) = 0$. We let $[x]_i$ denote the ith element of vector x.

We consider stochastic processes with respect to a probability space $(\Omega, \mathcal{F}, Pr)$, where Ω is a sample space, $\mathcal{F}$ is a σ-field over Ω, and $Pr : \mathcal{F} \to [0, 1]$ is a probability measure. A *filtration* $\{\mathcal{F}_t : t \geq 0\}$ is a collection of sub-σ-fields with $\mathcal{F}_s \subseteq \mathcal{F}_t \subseteq \mathcal{F}$ for $0 \leq s < t < \infty$. A stochastic process is *adapted* to filtration $\{\mathcal{F}_t\}$ if, for each $t \geq 0$, X_t is an $\mathcal{F}_t$-measurable random variable (Karatzas & Shreve, 2012).

Definition 1. The random process x_t is a *martingale* if $\mathbf{E}(x_t|x_s) = x_s$ for all $t \geq s$, a *submartingale* if $\mathbf{E}(x_t|x_s) \geq x_s$ for all $t \geq s$, and a *supermartingale* if $\mathbf{E}(x_t|x_s) \leq x_s$ for all $t \geq s$.

A stopping time is defined as follows.

Definition 2. A random time τ is a stopping time of a filtration $\mathcal{F}_t$ if the event $\{\tau \leq t\}$ belongs to the σ-field $\mathcal{F}_t$ for all $t \geq 0$.

Let x_t be a submartingale (resp. supermartingale) and let τ be a stopping time. If $t \wedge \tau$ denotes the minimum of t and τ, then $x_{t \wedge \tau}$ is a submartingale (resp. supermartingale). The following result gives bounds on the maximum value of a submartingale.

Theorem 1 (*Doob's Martingale Inequality* Karatzas & Shreve, 2012). *Let x_t be a submartingale, $[t_0, t_1]$ a subinterval of $[0, \infty)$, and $\lambda > 0$. Then*

$$\lambda Pr \left(\sup_{t_0 \leq t \leq t_1} x_t \geq \lambda \right) \leq \mathbf{E}(x_{t_1}^+). \tag{1}$$

The following result follows directly from Doob's Martingale Inequality.

Corollary 1. *Let x_t be a supermartingale, $[t_0, t_1]$ a subinterval of $[0, \infty)$, and $\lambda > 0$. Then*

$$\lambda Pr \left(\inf_{t \in [t_0, t_1]} x_t \leq -\lambda \right) \leq \mathbf{E}(x_{t_1}^+) - \mathbf{E}(x_{t_1}). \tag{2}$$

Proof. Since x_t is a supermartingale, $-x_t$ is a submartingale. Applying (1) with the submartingale $-x_t$ completes the proof. $\square$

The *quadratic variation* $\langle X \rangle$ of a random process X is the unique adapted increasing process for which $\langle X \rangle_0 = 0$ and $X^2 - \langle X \rangle$ is a martingale (Karatzas & Shreve, 2012).

We next define a semimartingale and give a composition result on semimartingales.

Definition 3. A continuous semimartingale x_t is a stochastic process which has decomposition $x_t = x_0 + M_t + A_t$ with probability 1, where M_t is a martingale and A_t is the difference between two continuous, nondecreasing, adapted processes.

For any stopping time τ and semimartingale x_t, $x_{t \wedge \tau}$ is a semimartingale. The following lemma gives a composition rule for semimartinigales.

Lemma 1 (Itô's Lemma Karatzas & Shreve, 2012)**.** *Let $f(x, t)$ be a twice-differentiable function and let x_t be a semimartingale. Then $f(x_t)$ is a semimartingale that satisfies*

$$f(x_t) = f(x_0) + \int_0^t f'(x_s) \, dM_s + \int_0^t f'(x_s) \, dA_s$$
$$+ \frac{1}{2} \int_0^t f''(x_s) \, d\langle M \rangle_s$$

with probability 1 for all t.

A stochastic differential equation (SDE) in Itô form is defined by

$$dx_t = a(x, t) \, dt + \sigma(x, t) \, dW_t \tag{3}$$

where $a(x, t)$ and $\sigma(x, t)$ are continuous functions and W_t is a Brownian motion. The dimension of x_t is equal to n, while the dimension of W_t is equal to q. A strong solution to an SDE is defined as follows.

Definition 4. A strong solution of SDE (3) with respect to Brownian motion W_t and initial condition χ is a process $\{x_t : t \in [0, \infty)\}$ with continuous sample paths and the following properties:

  (i) $Pr(x_0 = \chi) = 1$
  (ii) For every $1 \le i \le n$, $1 \le j \le r$, and $t \in [0, \infty)$,

$$Pr \left(\int_0^t |a_i(x_\tau, \tau)| + \sigma_{ij}^2(x_\tau, \tau) \, d\tau < \infty \right) = 1.$$

  (iii) The integral equation

$$x_t = x_0 + \int_0^t a(\tau, x_\tau) \, d\tau + \int_0^t \sigma(\tau, x_\tau) \, dW_\tau,$$

  where the latter term is a stochastic integral with respect to the Brownian motion W_t, holds with probability 1.

Any strong solution of an SDE is a semimartingale. For such strong solutions, if $f(x, t)$ is a twice differentiable function and $z_t = f(x_t, t)$, then Itô's Lemma reduces to

$$dz_t =$$
$$\left(\frac{\partial f}{\partial t} + \frac{\partial f}{\partial x} a(x, t) + \frac{1}{2} \mathbf{tr} \left(\sigma(x, t)^T \frac{\partial^2 f}{\partial x^2} \sigma(x, t) \right) \right) dt$$
$$+ \left(\frac{\partial f}{\partial x} \sigma(x, t) \right) dW_t \tag{4}$$

4. Complete-information CBFs

This section presents our construction of control barrier functions for stochastic systems where the controller has complete state information.

4.1. Problem statement

We consider a system with time-varying state $x_t \in \mathbb{R}^n$ and control input $u_t \in \mathbb{R}^m$. The state x_t follows the SDE

$$dx_t = (f(x_t) + g(x_t)u_t) \, dt + \sigma(x_t) \, dW_t \tag{5}$$

where $f : \mathbb{R}^n \to \mathbb{R}^n$, $g : \mathbb{R}^n \to \mathbb{R}^{n \times m}$, and $\sigma : \mathbb{R}^n \to \mathbb{R}^q$ are locally Lipschitz continuous functions and W_t is a Brownian motion. We assume that (5) has a strong solution for any control signal u_t.

The system is required to satisfy a safety constraint for all time t, which is expressed as $x_t \in \mathcal{C}$ for all t where $\mathcal{C}$ is a safe operating region. The set $\mathcal{C}$ is defined by a locally Lipschitz function $h : \mathbb{R}^n \to \mathbb{R}$ as

$$\mathcal{C} = \{x : h(x) \ge 0\}, \quad \partial\mathcal{C} = \{x : h(x) = 0\}.$$

The set of interior points of $\mathcal{C}$ is denoted as $\text{int}(\mathcal{C})$.

Problem studied: How to design a control policy that maps the sequence $\{x_{t'} : t' \in [0, t)\}$ to an input u_t such that $x_t \in \mathcal{C}$ for all t with probability 1?

We observe that, for systems where it is not possible to design a policy that ensures safety with probability 1, there may be policies that provide policy with some probability $\epsilon \in (0, 1)$. Constructing such policies is a direction for future work.

4.2. Reciprocal control barrier function construction

We present our first stochastic CBF construction, which is a *reciprocal* CBF (RCBF) analogous to Ames et al. (2016).

Definition 5. Let x_t be a stochastic process described by (5). A reciprocal CBF is a function $B : \mathbb{R}^n \to \mathbb{R}$ that is locally Lipschitz, twice differentiable on $\text{int}(\mathcal{C})$, and satisfies the following properties:

  (1) There exist class-K functions α_1 and α_2 such that

$$\frac{1}{\alpha_1(h(x))} \le B(x) \le \frac{1}{\alpha_2(h(x))} \tag{6}$$

  for all $x \in \text{int}(\mathcal{C})$.
  (2) There exists a class-K function α_3 such that, for all $x \in \text{int}(\mathcal{C})$, there exists $u \in \mathbb{R}^m$ such that

$$\frac{\partial B}{\partial x}(f(x) + g(x)u) + \frac{1}{2} \mathbf{tr} \left(\sigma(x)^T \frac{\partial^2 B}{\partial x^2} \sigma(x) \right)$$
$$\le \alpha_3(h(x)) \tag{7}$$

In the deterministic case (Ames et al., 2016), the reciprocal CBF construction ensures that $B(x)$ tends to infinity as the system state approaches the boundary of the safe region $\mathcal{C}$. Definition 5 extends this approach to the stochastic case by providing sufficient conditions for the system to remain bounded in expectation, and hence almost surely finite, as shown by the following theorem.

Theorem 2. *Suppose that there exists an RCBF B for a controlled stochastic process x_t described by (5), and at each time t, u_t satisfies (7). Then $Pr(x_t \in \mathcal{C} \ \forall t) = 1$, provided that $x_0 \in \mathcal{C}$.*

The proof is omitted due to space constraints. Theorem 2 implies that, by choosing u_t at each time t to satisfy (7), safety is guaranteed with probability 1.

4.3. Zero control barrier function construction

An alternative construction for CBFs is the *zero-CBF* (ZCBF). The deterministic ZCBF ensures that $\frac{dh}{dt} = 0$ when $h(x) = 0$, so that the system does not enter the unsafe area. Ensuring that

$\frac{dh}{dt} = 0$, however, may be inadequate in the presence of stochastic noise. We present a zero-CBF construction for stochastic systems that generalizes the construction in the deterministic case by using the Itô derivative instead of the Lie derivative.

Definition 6. The function $h(x)$ serves as a zero-CBF for a system described by SDE (5) if for all x satisfying $h(x) > 0$, there is a u satisfying

$$\frac{\partial h}{\partial x}(f(x) + g(x)u) + \frac{1}{2}\mathbf{tr}\left(\sigma^T \frac{\partial^2 h}{\partial x^2}\sigma\right) \geq -h(x) \tag{8}$$

We next state the main result on safety via zero-CBFs.

Theorem 3. If u_t satisfies (8) for all t, then $Pr(x_t \in \mathcal{C} \ \forall t) = 1$, provided $x_0 \in \mathcal{C}$.

Proof. We will show that, for all t, $Pr(x_{t'} \in \mathcal{C} \ \forall t' < t) = 1$, and hence

$$Pr(x_t \in \mathcal{C} \ \forall t) = \lim_{t \to \infty} Pr(x_{t'} \in \mathcal{C} \ \forall t' \in [0, t]) = 1.$$

It is sufficient to show that, for any $t > 0$, any $\epsilon > 0$, and any $\delta \in (0, 1)$,

$$Pr\left(\inf_{t' < t} h(x_{t'}) < -\epsilon\right) < \delta.$$

Let $\theta = \min\left\{\frac{\delta\epsilon}{2t}, h(x_0)\right\}$. By Itô's Lemma, we have that $h(x_t)$ is given by

$$h(x_t) = h(x_0) + \int_0^t \frac{\partial h}{\partial x}(f(x_\tau) + g(x_\tau)u_\tau)$$
$$+ \frac{1}{2}\mathbf{tr}\left(\sigma(x_\tau)^T \frac{\partial^2 h}{\partial x^2}\sigma(x_\tau)\right) d\tau$$
$$+ \int_0^t \sigma(x_\tau)\frac{\partial h}{\partial x} dW_\tau \tag{9}$$

We construct a sequence of stopping times η_i and ζ_i for $i = 0, 1, \ldots$ as

$$\eta_0 = 0, \quad \zeta_0 = \inf\{t : h(x_t) > \theta\}$$
$$\eta_i = \inf\{t : h(x_t) < \theta, t > \zeta_{i-1}\}, i = 1, 2, \ldots,$$
$$\zeta_i = \inf\{t : h(x_t) > \theta, t > \eta_{i-1}\}, i = 1, 2, \ldots,$$

The stopping times η_i and ζ_i are the down- and up-crossings of $h(x_t)$ over θ, respectively. Define a random process U_t as follows. Let $U_0 = \theta$, and let U_t be given by

$$U_t = U_0 + \sum_{i=0}^{\infty}\left[\int_{\eta_i \wedge t}^{\zeta_i \wedge t} -\theta \, d\tau + \int_{\eta_i \wedge t}^{\zeta_i \wedge t} \sigma \frac{\partial h}{\partial x} dW_\tau\right]. \tag{10}$$

We have that U_t is a semimartingale. Furthermore, we have

$$\mathbf{E}(U_t | U_s) = U_s + \mathbf{E}\left(\sum_{i=0}^{\infty}\left[\int_{\eta_i \wedge t}^{\zeta_i \wedge t} -\theta \, d\tau\right.\right.$$
$$\left.\left. + \int_{\eta_i \wedge t}^{\zeta_i \wedge t} \sigma \frac{\partial h}{\partial x} dW_\tau\right]\right)$$
$$= U_s + \mathbf{E}\left(\sum_{i=0}^{\infty}\int_{\eta_i \wedge t}^{\zeta_i \wedge t} -\theta \, d\tau\right) \leq U_s$$

and therefore U_t is a supermartingale.

We will first prove by induction that $h(x_t) \geq U_t$ and $U_t \leq \theta$. Initially, $U_0 = \theta \leq h(x_0)$ by construction. Suppose the result holds up to time $t \in [\eta_i, \zeta_i]$ for $i \geq 0$. Then the first term of (9) is an upper bound on the first term of (10) and the third terms are

equal. For $t \in [\eta_i, \zeta_i]$, $h(x_t)$ and U_t are given by

$$h(x_t) = h(x_{\eta_i}) + \int_{\eta_i}^t \left[\frac{\partial h}{\partial x}(f(x_\tau) + g(x_\tau)u\right.$$
$$\left. + \frac{1}{2}\mathbf{tr}\left(\sigma^T \frac{\partial^2 h}{\partial x^2}\sigma\right)\right] d\tau + \int_{\eta_i}^t \sigma \frac{\partial h}{\partial x} dW_\tau \tag{11}$$

$$U_t = U_{\eta_i} + \int_{\eta_i}^t -\theta \, d\tau + \int_{\eta_i}^t \sigma \frac{\partial h}{\partial x} dW_\tau. \tag{12}$$

We have that $U_{\eta_i} \leq h(x_{\eta_i}) = \theta$ by induction, and the third terms of (11) and (12) are equal. Since $h(x_t) \leq \theta$ for $t \in [\eta_i, \zeta_i]$, Eq. (8) implies

$$\frac{\partial h}{\partial x}(f(x) + g(x)u) + \frac{1}{2}\mathbf{tr}\left(\sigma^T \frac{\partial^2 h}{\partial x^2}\sigma\right)$$
$$\geq -h(x) \geq -\theta$$

so that the integrand of the second term of (11) is an upper bound on the integrand of the second term of (12). Hence $h(x_t) \geq U_t$. Furthermore, for $t \in [\eta_i, \zeta_i]$, $h(x_t) \leq \theta$, and thus $U_t \leq \theta$.

For $t \in [\zeta_i, \eta_{i+1}]$, we have that

$$U_t = U_{\zeta_i} \leq h(x_{\zeta_i}) = \theta \leq h(x_t)$$

by definition of ζ_i.

Since $U_t \leq h(x_t)$, we have that

$$Pr\left(\inf_{t' < t} h(x_{t'}) < -\epsilon\right) \leq Pr\left(\inf_{t' < t} U_{t'} < -\epsilon\right).$$

Corollary 1 implies that

$$\epsilon Pr\left(\inf_{t' < t} U_{t'} < -\epsilon\right) \leq \mathbf{E}(U_t^+) - \mathbf{E}(U_t).$$

The expectation of U_t is bounded as follows. Taking expectation of both sides of (10) yields

$$\mathbf{E}(U_t) = U_0 + \mathbf{E}\left[\sum_{i=0}^{\infty}\int_{\eta_i \wedge t}^{\zeta_i \wedge t} -\theta \, d\tau\right].$$

Since $\theta > 0$, the second term is bounded below by $-\theta t$, and so we have $\mathbf{E}(U_t) \geq \theta - \theta t$. Since $U_t \leq \theta$, we have $\mathbf{E}(U_t^+) \leq \theta$. Combining these yields

$$\mathbf{E}(\overline{U}_t^+) \leq \theta t - \theta + \theta = \theta t.$$

We therefore have

$$Pr\left(\inf_{t' < t} h(x_{t'}) < -\epsilon\right) \leq Pr\left(\inf_{t' < t} U_{t'} < -\epsilon\right)$$
$$\leq \frac{\theta t}{\epsilon} \leq \frac{\delta\epsilon}{2t}\frac{t}{\epsilon} < \delta,$$

completing the proof. □

4.4. High relative degree systems

The safety guarantees of the preceding section rely on the existence of a control input satisfying (7) and (8) at each time t. The conditions (7) and (8), however, may fail if $\frac{\partial h}{\partial x}g(x) = 0$. In systems with high relative degree, however, it may be the case that $\frac{\partial h}{\partial x}g(x) = 0$ for some x, potentially preventing the system from satisfying the conditions and rendering the safety guarantees inapplicable. We propose an approach to construct ZCBFs for such high-degree systems. We define a set of functions $h_i(x)$ for $i = 0, 1, \ldots$, as $h_0(x) = h(x)$,

$$h_{i+1}(x) = \frac{\partial h_i}{\partial x}f(x) + \frac{1}{2}\mathbf{tr}\left(\sigma^T \left(\frac{\partial^2 h_i}{\partial x^2}\right)\sigma\right) + h_i(x). \tag{13}$$

This approach is similar to the high relative degree stochastic RCBF construction presented in Sarkar, Ghose, and Theodorou (2020), albeit for stochastic ZCBF. Define $\mathcal{C}_i = \{x : h_i(x) \geq 0\}$ and, for any $r \geq 0$, let

$$\bar{\mathcal{C}}_r = \bigcap_{i=0}^{r} \mathcal{C}_i.$$

Theorem 4. *Suppose that there exists r such that, for any $x \in \bar{\mathcal{C}}_r$, we have $\frac{\partial h_i}{\partial x} g(x) \geq 0$ for $i < r$ and*

$$\frac{\partial h_r}{\partial x}(f(x) + g(x)u) + \frac{1}{2}\mathbf{tr}\left(\sigma^T \frac{\partial^2 h_r}{\partial x^2}\sigma\right) \geq -h_r(x). \qquad (14)$$

Then $Pr(x_t \in \mathcal{C} \ \forall t) = 1$ if $x_0 \in \bar{\mathcal{C}}_r$.

Proof. Suppose that u_t satisfying the conditions of the theorem is chosen at each time t. By Theorem 3, (14) implies that $h_r(x_t) \geq 0$ for all t. By definition of $h_r(x)$ and the assumption that $\frac{\partial h_{r-1}}{\partial x}g(x)u \geq 0$, we also have $h_{r-1}(x_t) \geq 0$ for all t. Proceeding inductively, we then have $h_i(x_t) \geq 0$ for all $i = 0, \ldots, r$, and hence in particular $h(x_t) = h_0(x_t) \geq 0$ for all t. $\square$

In what follows, we show that the conditions of Theorem 4 can be satisfied for an important subclass of systems, namely, controllable linear systems in which the safety constraint can be expressed as a half-plane. For such systems we have $f(x) = Fx$ and $g(x) = G$ for some matrices F and G, and the function $h(x) = a^T x - b$ for some $a \in \mathbb{R}^n$ and $b \in \mathbb{R}$. Since the system is controllable, we have $a^T F^i G \neq 0$ for some i. The following lemma describes the structure of the h_i's.

Lemma 2. *The function $h_i(x)$ can be written in the form*

$$h_i(x) = \sum_{r_0, \ldots, r_{i-1}} \beta_i^{r_0, \ldots, r_{i-1}, 0}(a^T F^0 x)^{r_0} \cdots (a^T F^{i-1}x)^{r_{i-1}}$$
$$+ a^T F^i x$$

for some values of the coefficients $\beta_i^{r_0, \ldots, r_i}$.

The proof is omitted due to space constraints. Define $r' = \min\{l : a^T F^l G \neq 0\}$. By the preceding lemma, we have, for any $x \in \bar{\mathcal{C}} \triangleq \bigcap_{i=0}^{r'} \mathcal{C}_i$,

$$\frac{\partial h_i}{\partial x}Gu = \begin{cases} 0, & i < r' \\ a^T F^r Gu, & i = r' \end{cases} \qquad (15)$$

We are now ready to state the safety result for high relative degree LTI systems.

Theorem 5. *Let $r = r'$. If $x_0 \in \bar{\mathcal{C}}$ and*

$$\frac{\partial h_r}{\partial x}g(x)u \geq -\frac{\partial h_r}{\partial x}f(x) - \frac{1}{2}\mathbf{tr}\left(\sigma^T \frac{\partial^2 h_r}{\partial x^2}\sigma\right) - h_r(x) \qquad (16)$$

for all t, then $Pr\left(x_t \in \bar{\mathcal{C}}\right) = 1$. In particular, x_t satisfies the safety constraint $\{h(x_t) > 0\}$ with probability 1.

Proof. By Theorem 4, it suffices to show that (14) holds and $\frac{\partial h_i}{\partial x}g(x)u_t \geq 0$ for all $i < r$. Eq. (14) holds by Eq. (16), and $\frac{\partial h_i}{\partial x}g(x) = 0$ for $i < r$ by (15). $\square$

5. Incomplete information CBFs

This section presents CBF techniques for ensuring safety of stochastic systems with incomplete information due to noisy measurements. We give the problem statement followed by RCBF and ZCBF constructions.

5.1. Problem statement

We consider a system with time-varying state $x_t \in \mathbb{R}^n$, a control input $u_t \in \mathbb{R}^m$, and output $y_t \in \mathbb{R}^p$ described by the SDEs

$$dx_t = (f(x_t) + g(x_t)u_t) \, dt + \sigma_t \, dV_t \qquad (17)$$
$$dy_t = b(x_t) \, dt + v_t \, dW_t \qquad (18)$$

where V_t and W_t are Brownian motions and $f : \mathbb{R}^n \to \mathbb{R}^n$, $g : \mathbb{R}^n \to \mathbb{R}^m$, and $b : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^p$ are locally Lipschitz continuous functions. Define $\bar{f}(x, u) = f(x) + g(x)u$. Note that, unlike in the complete information case, we assume that σ_t and v_t do not depend on x_t. This assumption is needed to ensure the existence of bounds on the estimation accuracy.

In the incomplete case, our CBF approaches are in two parts. First, we compute an estimate of the system state and construct a safe region for the estimated state based on the accuracy of the estimator. Second, we show that the problem reduces to a complete-information stochastic SDE on the estimated state value and apply the approaches developed in Section 4.

Definition 7 (*Reif, Gunther, Yaz, & Unbehauen, 2000*)**.** The pair $\left[\frac{\partial \bar{f}}{\partial x}(x, u), \frac{\partial b}{\partial x}(x)\right]$ is uniformly detectable if there exist a bounded, matrix-valued function $\Lambda(x)$ and a real number $\rho > 0$ such that

$$w^T\left(\frac{\partial \bar{f}}{\partial x}(x, u) + \Lambda(x)\frac{\partial b}{\partial x}(x)\right)w \leq -\rho\|w\|^2$$

for all w, z, and x.

Uniform detectability is a standard requirement for bounding the error of estimators such as the Extended Kalman Filter (Jazwinski, 2007; Li, Wei, Ding, Liu, & Alsaadi, 2016; Reif et al., 2000). Note that uniform detectability and detectability are equivalent for LTI systems.

The safety condition is defined as in Section 4.1. In the incomplete information case, the problem studied is stated as, *For given $\epsilon \in (0, 1)$, how to design a control policy that maps the sequence $\{y_{t'} : t' \in [0, t)\}$ to an input u_t at each time t such that $Pr(x_t \in \mathcal{C} \ \forall t) \geq (1 - \epsilon)$?* In other words, how to ensure that the system remains safe with a given probability $(1 - \epsilon)$?

We use the Extended Kalman Filter (EKF) (Reif et al., 2000) as a state estimator. Let $\hat{x}_t$ denote the estimated value of x_t, and define matrix A_t by

$$A_t = \frac{\partial \bar{f}}{\partial x}(\hat{x}_t, u_t).$$

Let $c_t = \frac{\partial b}{\partial x}(\hat{x}_t)$, $R_t = v_t v_t^T$, $Q_t = \sigma_t \sigma_t^T$, and P_t be equal to the solution to the Riccati differential equation

$$\frac{dP}{dt} = A_t P_t + P_t A_t^T + Q_t - P_t c_t^T R_t^{-1} c_t P_t.$$

The EKF estimator is defined by the SDE

$$d\hat{x}_t = f(\hat{x}_t, u_t) \, dt + K_t(dy_t - c_t \hat{x}_t \, dt). \qquad (19)$$

where $K_t = P_t c_t R_t^{-1}$ is the Kalman filter gain. Under this approach, the estimation error $\zeta_t = x_t - \hat{x}_t$ evolves according to the SDE

$$d\zeta_t = ((A_t - K_t c_t)\zeta_t + n_t) \, dt + \Gamma_t \begin{pmatrix} dV_t \\ dW_t \end{pmatrix},$$

where

$$n_t = \phi(x_t, \hat{x}_t, u_t) - K_t \chi(x_t, \hat{x}_t) \qquad (20)$$
$$\Gamma_t = \sigma_t - K_t v_t \qquad (21)$$

We make the following additional assumptions on the system dynamics to ensure stability of the EKF.

Assumption 1. The SDEs (17) and (18) satisfy:

(1) There exist constants $q, r \in \mathbb{R}_{\geq 0}$ such that $\sigma_t \sigma_t^T \geq qI$ and $v_t v_t^T \geq rI$ for all x and t.[1]

(2) The pair $\left[\frac{\partial \bar{f}}{\partial x}(x, u), \frac{\partial b}{\partial x} \right]$ is uniformly detectable.

(3) There exist real numbers ϵ_ϕ, k_ϕ, ϵ_χ, k_χ such that the functions ϕ and χ in (20) and (21) are bounded by

$$\|\phi(x, \hat{x}, u)\| \leq k_\phi \|x - \hat{x}\|^2$$
$$\|\chi(x, \hat{x})\| \leq k_\chi \|x - \hat{x}\|^2$$

for $x, \hat{x}$ satisfying $\|x - \hat{x}\|_2 \leq \epsilon_\phi$, $\|x - \hat{x}\| \leq \epsilon_\chi$.

The first assumption states that $\mathbf{E}(\sigma_t \sigma_t^T) \geq qI$ and $\mathbf{E}(v_t v_t^T) \geq rI$ for some q, r, and implies that the noise matrices are uniformly bounded below. The uniform detectability assumption ensures that all of the system modes can be observed, and that the covariance of the filter can be bounded, which is necessary for deriving error bounds. The third assumption states that the linearized approximation to $\bar{f}$ is approximately accurate in a neighborhood of x and $\hat{x}$. We further assume that the initial state x_0 is known. The following result describes the stability and accuracy of the EKF.

Proposition 1. *Suppose that the conditions of Assumption 1 hold, and that there exists $\bar{c}$ such that $\|c_t\|_2 \leq \bar{c}$ for all t. There exists $\delta > 0$ such that if $\sigma_t \sigma_t^T \leq \delta I$ and $v_t v_t^T \leq \delta I$, then for any $\epsilon > 0$, there exists $\gamma > 0$ with*

$$Pr\left(\sup_{t \geq 0} \|x_t - \hat{x}_t\|_2 \leq \gamma \right) \geq 1 - \epsilon. \tag{22}$$

We make two remarks on Proposition 1. First, the accuracy guarantees of the EKF do not depend on the magnitude of the control input u_t. Second, if the system is highly nonlinear, then the constant $\delta > 0$ may be small (Reif et al., 2000), rendering the results inapplicable. The following lemma considers the special case of LTI systems.

Lemma 3. *Suppose that $f(x_t) = Fx_t$ and $g(x_t) = G$ for some matrices F and G such that (F, G) is detectable. Let $\lambda^* = \sup_t \lambda_{max}(P_t)$, where $\lambda_{max}(\cdot)$ denotes the maximum eigenvalue of a matrix. Let $\gamma = \sqrt{\frac{n\lambda^*}{\epsilon}}$. Then $Pr(x_t \in \mathcal{C} \; \forall t) \geq (1 - \epsilon)$.*

The proof of this lemma appears in the preliminary conference version of this paper (Clark, 2019) and is omitted due to space constraints.

Define $\bar{h}(x) = \inf \{h(\hat{x}) : \|x - \hat{x}\|_2 \leq \gamma\}$. We have that, if $\bar{h}(\hat{x}_t) \geq 0$ and $\|x_t - \hat{x}_t\|_2 \leq \gamma$ for all t, then $h(x_t) \geq 0$ for all t. When $\bar{h}(x)$ is difficult to compute or non-differentiable, define

$$\bar{h}_\gamma = \sup \{h(x) : \|x - x^0\|_2 \leq \gamma \text{ for some } x^0 \in h^{-1}(\{0\})\}.$$

The following lemma gives a sufficient condition for safety of the incomplete information system.

Lemma 4. *If $\|x_t - \hat{x}_t\|_2 \leq \gamma$ for all t and $h(\hat{x}_t) > \bar{h}_\gamma$ for all t, then $x_t \in \mathcal{C}$ for all t.*

The proof is omitted due to space constraints. Combining Proposition 1 and Lemma 4, we have that it suffices to select γ such that $\|x_t - \hat{x}_t\|_2$ is bounded by γ with probability $(1 - \epsilon)$, and then design a control law such that $h(\hat{x}_t) > \bar{h}_\gamma$ for all t. Define $\hat{h}(x) = h(x) - \bar{h}_\gamma$.

---

[1] Here "$\geq$" refers to inequality in the semidefinite cone.

5.2. Reciprocal CBF approach

The RCBF for incomplete information systems is described as follows.

Theorem 6. *Suppose that the conditions of Proposition 1 are satisfied and there exist a function $B : \mathbb{R}^n \to \mathbb{R}$ and class-K functions α_1, α_2, and α_3 such that*

$$\frac{1}{\alpha_1(\hat{h}(x))} \leq B(x) \leq \frac{1}{\alpha_2(\hat{h}(x))} \tag{23}$$

$$\frac{\partial B}{\partial x} \bar{f}(\hat{x}_t, u_t) + \gamma \left\| \frac{\partial B}{\partial x} K_t c \right\|_2 + \frac{1}{2} \mathbf{tr} \left(v_t^T K_t^T \frac{\partial^2 B}{\partial x^2} K_t v_t \right)$$
$$\leq \alpha_3(\hat{h}(\hat{x}_t)) \tag{24}$$

and γ satisfies (22) for some $\epsilon > 0$. $Pr(x_t \in \mathcal{C} \; \forall t) \geq (1 - \epsilon)$ if $\hat{h}(x_0) > 0$.

Proof. We show that $\hat{h}(\hat{x}_t) \geq 0$ for all t if $\|x_t - \hat{x}_t\|_2 \leq \gamma$ for all t. Combining Eqs. (18) and (19) yields

$$d\hat{x}_t = \bar{f}(\hat{x}_t, u_t) \, dt + K_t(cx_t \, dt + v_t \, dW_t - c\hat{x}_t \, dt)$$
$$= (\bar{f}(\hat{x}_t, u_t) + K_t c(x_t - \hat{x}_t)) \, dt + K_t v_t \, dW_t$$

Define $B_t = B(\hat{x}_t)$. Hence

$$dB_t = \left(\frac{\partial B}{\partial x}(\bar{f}(\hat{x}_t, u_t) + K_t c(x_t - \hat{x}_t)) \right.$$
$$\left. + \frac{1}{2} \mathbf{tr} \left(v_t^T K_t^T \frac{\partial^2 B}{\partial x^2} K_t v_t \right) \right) dt + \frac{\partial B}{\partial x} K_t v_t \, dW_t \tag{25}$$

If $\|x_t - \hat{x}_t\|_2 \leq \gamma$, then

$$\frac{\partial B}{\partial x} K_t c(x_t - \hat{x}_t) \leq \left\| \frac{\partial B}{\partial x} K_t c \right\|_2 \|x_t - \hat{x}_t\|_2 \leq \gamma \left\| \frac{\partial B}{\partial x} K_t c \right\|_2.$$

Hence, if (24) holds, then

$$\frac{\partial B}{\partial x}(\bar{f}(\hat{x}_t, u_t) + K_t c(x_t - \hat{x}_t)) + \frac{1}{2} \mathbf{tr} \left(v_t^T K_t^T \frac{\partial^2 B}{\partial x^2} K_t v_t \right)$$
$$\leq \frac{\partial B}{\partial x} \left(\bar{f}(\hat{x}_t, u_t) + \gamma \left\| \frac{\partial B}{\partial x} K_t c \right\|_2 \right)$$
$$+ \frac{1}{2} \mathbf{tr} \left(v_t^T K_t^T \frac{\partial^2 B}{\partial x^2} K_t v_t \right) \leq \alpha_3(\hat{h}(\hat{x}_t))$$

and thus $Pr(\hat{h}(\hat{x}_t) \geq 0 \; \forall t) = 1$ by Theorem 2. Hence, by Lemma 4, $Pr(h(x_t) \geq 0 \; \forall t | \|x_t - \hat{x}_t\|_2 \leq \gamma \; \forall t) = 1$, and so $Pr(h(x_t) \geq 0) \geq 1 - \epsilon$. $\square$

Theorem 6 implies that, if the parameter γ is chosen such that the estimation error remains bounded by γ with sufficient probability, then selecting a control input u_t at each time t such that (24) holds is sufficient to ensure safety. This constraint is linear in u_t, and all other parameters can be evaluated based on the noise characteristics and system and Kalman filter matrices.

5.3. Zero CBF construction

The following definition describes the zero CBF in the incomplete information case.

Definition 8. The function $\hat{h}(x)$ serves as a zero CBF for an incomplete-information system described by (17) and (18) if for all x satisfying $\hat{h}(x) > 0$, there exists u satisfying

$$\frac{\partial \hat{h}}{\partial x} g(x) u \geq -\frac{\partial \hat{h}}{\partial x} f(\hat{x}_t) + \left\| \frac{\partial \hat{h}}{\partial x} K_t c \right\|_2 \gamma$$
$$- \frac{1}{2} \mathbf{tr} \left(\sigma^T \frac{\partial^2 \hat{h}}{\partial x^2} \sigma \right) - \hat{h}(\hat{x}_t) \tag{26}$$

Table 1
Constraints for the CBF-based control policies in complete and information systems (Eqs. (31) and (32)).

Solution approach	Linear constraint Ω_t
RCBF, complete information	$\frac{\partial B}{\partial x}g(x_t)u_t \leq \alpha_3(h(x_t)) - \frac{\partial B}{\partial x}f(x_t) - \frac{1}{2}\mathbf{tr}\left(\sigma(x_t)^T\frac{\partial^2 B}{\partial x^2}\sigma(x_t)\right)$
ZCBF, complete information	$\frac{\partial h}{\partial x}g(x_t)u_t \geq -\frac{\partial h}{\partial x}f(x_t) - \frac{1}{2}\mathbf{tr}(\sigma^T\frac{\partial^2 h}{\partial x^2}\sigma) - h(x_t)$
RCBF, incomplete information	$\frac{\partial B}{\partial x}g(\hat{x}_t)u \leq \alpha_3(\hat{h}(\hat{x}_t)) - \frac{\partial B}{\partial x}f(\hat{x}_t) - \gamma\|\frac{\partial B}{\partial x}K_tc\|_2 - \frac{1}{2}\mathbf{tr}\left(v_t^T K_t^T \frac{\partial^2 B}{\partial x^2}K_t v_t\right)$
ZCBF, incomplete information	$\frac{\partial \hat{h}}{\partial x}g(x)u \geq -\frac{\partial \hat{h}}{\partial x}f(\hat{x}_t) + \|\frac{\partial \hat{h}}{\partial x}K_tc\|_2\gamma - \frac{1}{2}\mathbf{tr}\left(\sigma^T\frac{\partial^2 \hat{h}}{\partial x^2}\sigma\right) - \hat{h}(\hat{x}_t)$

The following theorem describes the safety guarantees of the incomplete-information ZCBF.

Theorem 7. *Suppose that x_0 satisfies $\hat{h}(x_0) > 0$ and, at each time t, u_t satisfies (26). If the conditions of Proposition 1 are satisfied, then $Pr(x_t \in \mathcal{C} \; \forall t) \geq (1 - \epsilon)$.*

Proof. Our approach is to show that $\hat{h}(\hat{x}_t) > 0$ for all t when $\|x_t - \hat{x}_t\|_2 \leq \gamma$, and hence safety is satisfied with probability at least $(1-\epsilon)$ by Lemma 4. The dynamics of $\hat{x}_t$ are given by the SDE (17). Note that

$$-\frac{\partial \hat{h}}{\partial \hat{x}}K_tc(x_t - \hat{x}_t) \leq \|\frac{\partial \hat{h}}{\partial \hat{x}}K_tc\|_2\|x_t - \hat{x}_t\|_2 \leq \|\frac{\partial \hat{h}}{\partial \hat{x}}K_tc\|_2\gamma. \quad (27)$$

We then have

$$-\frac{\partial \hat{h}}{\partial \hat{x}}\left(f(\hat{x}_t) + K_tc(x_t - \hat{x}_t)\right) - \frac{1}{2}\mathbf{tr}\left(\sigma^T\left(\frac{\partial^2 \hat{h}}{\partial \hat{x}^2}\right)\sigma\right) \quad (28)$$

$$\leq -\frac{\partial \hat{h}}{\partial \hat{x}}f(\hat{x}_t) + \|\frac{\partial \hat{h}}{\partial \hat{x}}K_tc\|_2\gamma - \frac{1}{2}\mathbf{tr}\left(\sigma^T\left(\frac{\partial^2 \hat{h}}{\partial \hat{x}^2}\right)\sigma\right) \quad (29)$$

$$\leq \frac{\partial \hat{h}}{\partial \hat{x}}g(\hat{x}_t)u_t \quad (30)$$

where (29) follows from (27) and (30) follows from (26). Hence, by Theorem 3, $h(\hat{x}_t) > 0$ for all t if $\|x_t - \hat{x}_t\|_2 \leq \gamma$ for all t, and thus $Pr(h(x_t) > 0 \; \forall t) \geq (1 - \epsilon)$. $\square$

6. CBF-based control policies

In what follows, we describe control policies that use stochastic CBFs to provide provable safety guarantees. We consider a case where the goal of the system is to minimize the expected value of a positive-definite quadratic objective function $V(x_t, u_t)$. In the complete information case, the controller input u_t at time t can be computed as the solution to the quadratic program

$$\begin{aligned}\text{minimize}_{u_t} \quad & V_t(x_t, u_t) \\ \text{s.t.} \quad & u_t \in \Omega_t(x_t)\end{aligned} \quad (31)$$

where the set $\Omega_t(x_t)$ is an affine subspace in u_t. The value of $\Omega_t(x_t)$ depends on whether the RCBF or ZCBF construction is used, as shown in Table 1.

In the incomplete information case, the controller contains an Extended Kalman Filter, which computes an estimate $\hat{x}_t$ of the state x_t as a function of the prior observations $\{y_\tau : \tau \in [0, t)\}$. The controller computes each control input u_t as a solution to the optimization problem

$$\min\{V_t(\hat{x}_t, u_t) : u_t \in \Omega_t(\hat{x}_t)\} \quad (32)$$

where $\Omega_t(\hat{x}_t)$ is an affine subspace in u_t. The values of $\Omega_t(\hat{x}_t)$ are shown in Table 1.

We observe that these quadratic programs can be extended to describe multiple safety constraints, for example, when the region $\mathcal{C} = \bigcap_{i=1}^{N}\{x : h_i(x) \geq 0\}$. This extension can be performed by having a set of linear constraints, one for each safety condition $\{h_i(x) \geq 0\}$. There is no guarantee, however, that such a program has a feasible solution u_t.

An advantage of the CBF method in the deterministic case is that CBFs can be composed with Control Lyapunov Functions to provide joint guarantees on safety and stability. Such CLFs are defined in the stochastic setting as follows.

Proposition 2 (*Florchinger, 1997*). *Suppose there exists a function $V : \mathbb{R}^n \to \mathbb{R}$ such that, for every x, there exists u satisfying*

$$\frac{\partial V}{\partial x}(f(x) + g(x)u) + \mathbf{tr}\left(\sigma^T\frac{\partial^2 V}{\partial x^2}\sigma\right) \leq 0 \quad (33)$$

If u_t is chosen to satisfy (33) at each time t, then 0 is stochastically asymptotically stable.

Proposition 2 implies that stability requirements can be incorporated as a linear constraint on the optimization-based control. Hence, if the control input can be chosen at each time t to jointly satisfy the appropriate CBF constraint of Table 1 and the CLF constraint (33), then the system is guaranteed to asymptotically approach the desired operating point while remaining safe for all time.

7. Numerical study

We performed a numerical study of a multi-agent collision avoidance scenario using Matlab. Our case study is based on Borrmann, Wang, Ames, and Egerstedt (2015). We considered a set of n agents, indexed $i = 1, \ldots, n$, where agent i has position and velocity $[p_t]_i$ and $[v_t]_i$ with $d[p_t]_i = [v_t]_i \, dt + \sigma_p \, dW_t$ and $d[v_t]_i = [u_t]_i \, dt + \sigma_v \, dW_t$. The agents were uniformly placed on a circle of radius $\rho = 150$, with each agent attempting to travel to the opposite point on the circle while avoiding collisions. Each pair of agents (i, j) had a safety constraint

$$h_{ij} = \|p_i - p_j\|_2 - D_s \geq 0,$$

where $D_s = 10$. The sensor measurements satisfied $dy_t = x_t \, dt + v \, dW_t$ where $v = I$. We set $\sigma_p = \sigma_v = I$. The cost function to be minimized was equal to $\|u - \bar{u}\|_2$, where $\bar{u}$ is obtained using a linear control law $\bar{u}_t = -k_1([p_t]_i - [r]_i) - k_2[v_t]_i$. The CBF constraints were constructed using the method for high relative degree systems introduced in Section 4.4. We compared our approach with a simplified CBF-based controller, in which a deterministic CBF constraint of the form in Ames et al. (2019) is applied to the state estimate $\hat{x}_t$ obtained using the Kalman filter.

The agent trajectories are shown in Fig. 2(a). Each agent moves to reach the desired destination while avoiding collisions. We observe that all agents avoid traversing the center in order to minimize collisions. Fig. 2(b) shows the gap between the desired and actual control input over time. The proposed stochastic ZCBF led to a reduced deviation from the desired control input compared to the simplified CBF.

The minimum distances achieved by the three policies are shown in Fig. 2(c). The linear control law leads to safety violations as the agents attempt to reach their desired final positions while disregarding safety. The CBF-based approaches both avoid safety violations, with the stochastic ZCBF approaching the unsafe region before recovering to maintain a safe distance and still converging to the desired final position.
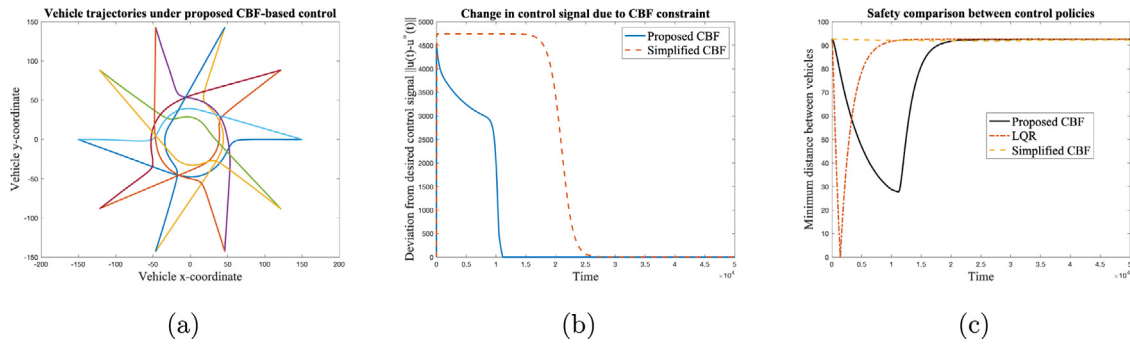
(a) (b) (c)

Fig. 2. Evaluation of stochastic CBFs using multi-agent collision avoidance. Ten agents are initially placed equidistant on a circle and must reach the opposite point without colliding in the presence of process and measurement noise. We compare our stochastic ZCBF approach with a proportional linear control law that does not incorporate safety, as well as a simplified CBF that uses the deterministic CBF of Ames et al. (2016) on the estimated state. (a) The agent trajectories. Each agent has double-integrator dynamics and avoids the center of the circle to prevent collisions. (b) Comparison of the deviation between the control action chosen and the desired action under a linear control law. The simplified CBF leads to higher deviation compared to our proposed stochastic ZCBF. (c) The minimum distance between vehicles under the linear control law and two CBF-based approaches. The linear controller leads to safety violations, while the CBF-based approaches avoid collisions.

8. Conclusion

This paper developed a framework for safe control of stochastic systems via Control Barrier Functions. We considered two scenarios, namely, complete information in which the true state is known to the controller at each time, and incomplete information in which the controller only has access to sensor measurements that are corrupted by Gaussian noise. For each case, we constructed Reciprocal and Zero CBFs, which ensure that the system remains safe provided that the CBF is finite (RCBF) or nonnegative (ZCBF). We proved that both constructions guarantee safety with probability 1 in the complete information case, and provide stochastic safety guarantees that depend on the estimation accuracy in the incomplete information case. We proposed control policies that ensure safety and stability by solving quadratic programs containing CBFs and stochastic Control Lyapunov Functions (CLFs) at each time step. We evaluated our approach through a numerical simulation on a multi-agent collision avoidance scenario. Future work will consider techniques for more general high relative-degree systems, as well as systems that are not affine in the control input. Another direction for future work consists of exploring the distinctions between RCBF- and ZCBF-based control policies. For example, in the deterministic case, the fact that the ZCBF is well-defined even outside the safe region can be used to design controllers that converge to the safe region if the initial state is outside the safe region. Generalizing such results to the stochastic setting remains an open problem.

References

Althoff, Matthias, Le Guernic, Colas, & Krogh, Bruce H. (2011). Reachable set computation for uncertain time-varying linear systems. In *Proceedings of the 14th international conference on hybrid systems: computation and control* (pp. 93–102). ACM.

Ames, Aaron D., Coogan, Samuel, Egerstedt, Magnus, Notomista, Gennaro, Sreenath, Koushil, & Tabuada, Paulo (2019). Control barrier functions: Theory and applications. In *2019 18th European control conference (ECC)* (pp. 3420–3431). IEEE.

Ames, Aaron D., Grizzle, Jessy W., & Tabuada, Paulo (2014). Control barrier function based quadratic programs with application to adaptive cruise control. In *Decision and control (CDC), 2014 IEEE 53rd annual conference on* (pp. 6271–6278). IEEE.

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

Borrmann, Urs, Wang, Li, Ames, Aaron D., & Egerstedt, Magnus (2015). Control barrier certificates for safe swarm behavior. *IFAC-PapersOnLine*, 48(27), 68–73.

Chen, Yuxiao, Peng, Huei, & Grizzle, Jessy (2017). Obstacle avoidance for low-speed autonomous vehicles with barrier function. *IEEE Transactions on Control Systems Technology*, 26(1), 194–206.

Cheng, Richard, Khojasteh, Mohammad Javad, Ames, Aaron D., & Burdick, Joel W. (2020). Safe multi-agent interaction through robust control barrier functions with learned uncertainties. arXiv preprint arXiv:2004.05273.

Cheng, Richard, Orosz, Gábor, Murray, Richard M., & Burdick, Joel W. (2019). End-to-end safe reinforcement learning through barrier functions for safety-critical continuous control tasks. In *Proceedings of the AAAI conference on artificial intelligence, Vol. 33* (pp. 3387–3395).

Chutinan, Alongkrit (1999). *Hybrid system verification using discrete model approximations* (Ph. D. dissertation), Department of Electrical and Computer Engineering, Carnegie Mellon University.

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

Dolginova, Ekaterina, & Lynch, Nancy (1997). Safety verification for automated platoon maneuvers: A case study. In *International workshop on hybrid and real-time systems* (pp. 154–170). Springer.

Fan, David D., Nguyen, Jennifer, Thakker, Rohan, Alatur, Nikhilesh, Agha-mohammadi, Ali-akbar, & Theodorou, Evangelos A. (2020). Bayesian learning-based adaptive control for safety critical systems. In *2020 IEEE international conference on robotics and automation (ICRA)* (pp. 4093–4099). IEEE.

Florchinger, Patrick (1997). Feedback stabilization of affine in the control stochastic differential systems by the control Lyapunov function method. *SIAM Journal on Control and optimization*, 35(2), 500–511.

Girard, Antoine, Le Guernic, Colas, & Maler, Oded (2006). Efficient computation of reachable sets of linear time-invariant systems with inputs. In *International workshop on hybrid systems: computation and control* (pp. 257–271). Springer.

Hsu, Shao-Chen, Xu, Xiangru, & Ames, Aaron D. (2015). Control barrier function based quadratic programs with application to bipedal robotic walking. In *American control conference (ACC), 2015* (pp. 4542–4548). IEEE.

Jagtap, Pushpak, Soudjani, Sadegh, & Zamani, Majid (2020). Formal synthesis of stochastic systems via control barrier certificates. *IEEE Transactions on Automatic Control*.

Jahanshahi, Niloofar, Jagtap, Pushpak, & Zamani, Majid (2020). Synthesis of partially observed jump-diffusion systems via control barrier functions. *IEEE Control Systems Letters*, 5(1), 253–258.

Jankovic, Mrdjan (2018). Control barrier functions for constrained control of linear systems with input delay. In *2018 annual American control conference (ACC)* (pp. 3316–3321). IEEE.

Jazwinski, Andrew H. (2007). *Stochastic processes and filtering theory*. Courier Corporation.

Karatzas, Ioannis, & Shreve, Steven (2012). *Brownian motion and stochastic calculus, Vol. 113*. Springer Science & Business Media.

Khojasteh, Mohammad Javad, Dhiman, Vikas, Franceschetti, Massimo, & Atanasov, Nikolay (2020). Probabilistic safety constraints for learned high relative degree system dynamics. In *Learning for dynamics and control* (pp. 781–792).

Li, Wangyan, Wei, Guoliang, Ding, Derui, Liu, Yurong, & Alsaadi, Fuad E. (2016). A new look at boundedness of error covariance of Kalman filtering. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 48(2), 309–314.

Lindemann, Lars, & Dimarogonas, Dimos V. (2019). Control barrier functions for signal temporal logic tasks. *IEEE Control Systems Letters*, 3(1), 96–101.

Mehra, Aakar, Ma, Wen-Loong, Berg, Forrest, Tabuada, Paulo, Grizzle, Jessy W., & Ames, Aaron D. (2015). Adaptive cruise control: Experimental validation of advanced controllers on scale-model cars. In *2015 American control conference (ACC)* (pp. 1411–1418). IEEE.

Mitra, Sayan, Wongpiromsarn, Tichakorn, & Murray, Richard M. (2013). Verifying cyber-physical interactions in safety-critical systems. *IEEE Security & Privacy*, *11*(4), 28–37.

Nguyen, Quan, & Sreenath, Koushil (2016a). Exponential control barrier functions for enforcing high relative-degree safety-critical constraints. In *American control conference (ACC), 2016* (pp. 322–328). IEEE.

Nguyen, Quan, & Sreenath, Koushil (2016b). Optimal robust control for constrained nonlinear hybrid systems with application to bipedal locomotion. In *2016 American control conference (ACC)* (pp. 4807–4813). IEEE.

Prajna, Stephen, & Jadbabaie, Ali (2004). Safety verification of hybrid systems using barrier certificates. In *International workshop on hybrid systems: Computation and control* (pp. 477–492). Springer.

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

Ratschan, Stefan, & She, Zhikun (2005). Safety verification of hybrid systems by constraint propagation based abstraction refinement. In *International workshop on hybrid systems: Computation and control* (pp. 573–589). Springer.

Rauscher, Manuel, Kimmel, Melanie, & Hirche, Sandra (2016). Constrained robot control using control barrier functions. In *Intelligent robots and systems (IROS), 2016 IEEE/RSJ international conference on* (pp. 279–285). IEEE.

Reif, Konrad, Gunther, Stefan, Yaz, Engin, & Unbehauen, Rolf (2000). Stochastic stability of the continuous-time extended Kalman filter. *IEE Proceedings D (Control Theory and Applications)*, *147*(1), 45–52.

Romdlony, Muhammad Zakiyullah, & Jayawardhana, Bayu (2016). Stabilization with guaranteed safety using control Lyapunov–barrier function. *Automatica*, *66*, 39–47.

Santoyo, Cesar, Dutreix, Maxence, & Coogan, Samuel (2019). Verification and control for finite-time safety of stochastic systems via barrier functions. In *2019 IEEE conference on control technology and applications (CCTA)* (pp. 712–717). IEEE.

Sarkar, Meenakshi, Ghose, Debasish, & Theodorou, Evangelos A. (2020). High-relative degree stochastic control Lyapunov and barrier functions. arXiv preprint arXiv:2004.03856.

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

Tomlin, Claire, Pappas, George J., & Sastry, Shankar (1998). Conflict resolution for air traffic management: A study in multiagent hybrid systems. *IEEE Transactions on Automatic Control*, *43*(4), 509–521.

Wu, Guofan, & Sreenath, Koushil (2016). Safety-critical control of a planar quadrotor. In *2016 American control conference (ACC)* (pp. 2252–2258). IEEE.

Xiao, Wei, & Belta, Calin (2019). Control barrier functions for systems with high relative degree. In *2019 IEEE 58th conference on decision and control (CDC)* (pp. 474–479). IEEE.

Xu, Xiangru (2018). Constrained control of input–output linearizable systems using control sharing barrier functions. *Automatica*, *87*, 195–201.

Yang, Guang, Belta, Calin, & Tron, Roberto (2019). Self-triggered control for safety critical systems using control barrier functions. In *2019 American control conference (ACC)* (pp. 4454–4459). IEEE.

Andrew Clark is an Associate Professor in the Department of Electrical and Computer Engineering at Worcester Polytechnic Institute. He received the B.S. degree in Electrical Engineering and the M.S. degree in Mathematics from the University of Michigan - Ann Arbor in 2007 and 2008, respectively. He received the Ph.D. degree from the Network Security Lab (NSL), Department of Electrical Engineering, at the University of Washington - Seattle in 2014. He is author or co-author of the IEEE/IFIP William C. Carter award-winning paper (2010), the WiOpt Best Paper (2012), and the WiOpt Student Best Paper (2014), and was a finalist for the IEEE CDC 2012 Best Student-Paper Award. He received the GameSec Outstanding Paper Award (2018) and was finalist for the ACM ICCPS Best Paper Award (2016, 2018, 2020). He received the University of Washington Center for Information Assurance and Cybersecurity (CIAC) Distinguished Research Award (2012) and Distinguished Dissertation Award (2014) and an NSF CAREER award (2020). His research interests include control and security of complex networks, submodular optimization, and control-theoretic modeling of network security threats.