2019 American Control Conference (ACC)
Philadelphia, PA, USA, July 10-12, 2019

Control Barrier Functions for Complete and Incomplete Information Stochastic Systems

Andrew Clark

Abstract— **Real-time controllers must satisfy strict safety requirements. Recently, Control Barrier Functions (CBFs) have been proposed that guarantee safety by ensuring that a suitably-defined barrier function remains bounded for all time. The CBF method, however, has only been developed for deterministic systems and systems with worst-case disturbances and uncertainties. In this paper, we develop a CBF framework for safety of stochastic systems. We consider complete information systems, in which the controller has access to the exact system state, as well as incomplete information systems where the state must be reconstructed from noisy measurements. In the complete information case, we formulate a notion of barrier functions that leads to sufficient conditions for safety with probability 1. In the incomplete information case, we formulate barrier functions that take an estimate from an extended Kalman filter as input, and derive bounds on the probability of safety as a function of the asymptotic error in the filter. We show that, in both cases, the sufficient conditions for safety can be mapped to linear constraints on the control input at each time, enabling the development of tractable optimization-based controllers that guarantee safety, performance, and stability. Our approach is evaluated via simulation study on an adaptive cruise control case study.**

I. Introduction

Safety-critical systems in application domains including automobiles, aviation, energy, and medicine must satisfy strict requirements on their state trajectories in order to prevent economic harm and loss of life. These requirements must be satisfied by real-time controllers in the presence of disturbances and process and measurement noise. Reliance on distributed and embedded systems places further computational constraints on the control.

There has been extensive research into safety verification of control systems, which has grown increasingly salient with the emergence of autonomous cyber-physical systems. Common techniques include Lypaunov and barrier methods [1], [2], discrete approximations [3]–[5], and direct computation of reachable sets [6], [7], among others. In addition to proving safety of a given system and controller, there has been research interest in synthesizing controllers with provable safety guarantees.

One recently-proposed framework for safe control is the use of *Control Barrier Functions* (CBF) [8], [9]. A CBF takes as input the current system state and outputs a real number corresponding to the safety state of the system. As the system approaches an unsafe operating point, the CBF value increases to infinity. Safety of the system can therefore be guaranteed by designing a controller such that the CBF remains finite for all time.

The CBF framework provides several advantages in addition to provable safety guarantees. For affine control systems, CBFs lead to linear constraints on the control, which can be used to design computationally tractable optimization-based controllers. CBFs can be easily composed with control Lyapunov functions to provide joint guarantees on stability, performance, and safety. CBFs have been proposed for diverse applications including vehicle cruise control [9], bipedal locomotion [10], and control of multi-robot swarms [11].

Existing CBF techniques consider systems that are deterministic or have bounded disturbances, and in which the controller has access to the current state of the system. In many applications of interest, however, the system to be controlled is perturbed by noise in the dynamics, and can only be observed via noisy 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. Such a framework, however, is not available in the existing literature.

In this paper, we generalize CBF to stochastic systems. We consider complete information systems, in which the exact state value is known at each time step, as well as incomplete information systems in which only noisy measurements of the state are available. In both cases, we show that a linear constraint on the control at each time step results in provable probabilistic safety guarantees. We make the following specific contributions:

- In the complete information case, we formulate a notion of control barrier function and derive sufficient conditions for the system to satisfy safety constraints with probability 1.
- In the incomplete information case, we consider a class of controllers that are based on a state estimate obtained via an Extended Kalman Filter. We derive bounds on the probability of violating the safety constraints as a function of the steady-state estimation error of the filter, and bound the violation probability when the system dynamics are linear.
- We describe how to synthesize optimization-based controllers that compute the control action at each time step by solving quadratic programs. We remark on how stability and performance can be integrated via stochastic Control Lyapunov Functions.

A. Clark is with the Department of Electrical and Computer Engineering, Worcester Polytechnic Institute, Worcester, MA 01609, USA aclark@wpi.edu

This work was supported by NSF grants CNS-1544173 and CNS-1656981.

- Our results are illustrated via numerical study on an adaptive cruise control example. We find that our proposed CBF method ensures safety even when other deterministic CBF heuristics lead to safety violations.

The rest of the paper is organized as follows. Section II reviews related work. Section III presents needed background. Section IV considers the complete information case. Section V considers the incomplete-information case. Section VII presents simulation results. Section VIII concludes the paper.

II. Related Work

The problem of verifying safety of a given system and controller has received extensive research attention [3], [4], [12]–[14]. In the verification literature, the approach that is closest to the present work is the barrier function method [1], [2]. In this method, a barrier function is constructed that is bounded below by a given value in the unsafe region, and then the trajectory of the barrier function is analyzed to prove that the state trajectory does not enter the unsafe region. Existing works have developed methods, typically based on semidefinite programming, for constructing barrier functions for deterministic, hybrid, uncertain, and stochastic systems. These works, however, are focused on proving safety of a given controller, while the goal of the present paper is to synthesize a controller with safety guarantees.

The CBF method for synthesizing safe controllers was proposed in [8] and has since been considered in [9], [15]–[19]. These existing works, however, do not consider stochastic systems with noise in either the state dynamics or the system measurements. Furthermore, applying these existing methods on an estimated state value may be insufficient to ensure safety, as we demonstrate in the simulation study.

III. Background

We let $\mathbf{E}(\cdot)$ and $\mathbf{tr}(\cdot)$ denote expectation and trace, respectively. We first review the concepts of martingales and stopping times.

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 variable 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 $t \geq 0$.

Intuitively, a random time τ is a stopping time if all of the information required to decide if $\tau = t$ is available at time t. For example, for a random process X_t that is adapted to $\mathcal{F}_t$, $\tau = \min\{t : X_t = c\}$ is a stopping time for any constant c, but $\tau = \max\{t : X_t = c\}$ is not a stopping time.

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). In other words, stopped martingales are martingales. The following lemma gives a condition on the maximum value of a submartingale.

Lemma 1 (Doob's Martingale Inequality [20]): Let $(x_t, \mathcal{F}_t)$ be a submartingale, $[t_0, t_1]$ a subinterval of $[0, \infty)$, and $\lambda > 0$. Then

$$\lambda Pr\left(\sup_{t_0 \leq t \leq t_1} x_t \geq \lambda\right) \leq \mathbf{E}(\max\{x_t, 0\}) \tag{1}$$

Definition 3: A continuous semimartingale X_t is a process which has the decomposition $X_t = X_0 + M_t + B_t$ with probability 1, where M_t is a martingale and B_t is the difference of two continuous, nondecreasing, adapted processes.

A stopped semimartingale is also a semimartingale. The following lemma describes a composition rule for semimartingales.

Lemma 2 (Itô's Lemma [20]): 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

$$f(X_t) = f(X_0) + \int_0^t f'(X_s)\ dM_s + \int_0^t f'(X_s)\ dB_s + \frac{1}{2}\int_0^t f''(X_s) d < M >_s$$

with probability 1 for all t, where $< M >_s$ denotes the quadratic variation of M.

We will use the standard notation

$$dx_t = a(x,t)dt + \sigma(x,t)dW_t \tag{2}$$

to describe a stochastic differential equation (SDE) in Itô form, 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 r. The notion of a solution of (2) used in this paper is defined as follows.

Definition 4 ([20], Def. 5.2.1): A strong solution of the SDE (2) with respect to Brownian motion W and initial condition ξ is a process $\{x_t : t \in [0, \infty)\}$ with continuous sample paths and the following properties:

(i) $Pr(x_0 = \xi) = 1$

(ii) For every $1 \leq i \leq n$, $1 \leq j \leq r$, and $t \in [0, \infty)$,

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

(iii) The integral equation

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

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

Any strong solution of an SDE is a semimartingale [20]. For such strong solutions, if $f(x,t)$ is a twice differentiable function, then Itô's Lemma reduces to

$$dz_t = \left(\frac{\partial f}{\partial t} + \frac{\partial f}{\partial x}a(x,t) + \frac{1}{2}\mathbf{tr}\left(\sigma(x,t)^T \frac{\partial^2 f}{\partial x^2}\sigma(x,t)\right)\right)dt + \left(\frac{\partial f}{\partial x}\sigma(x,t)\right)dW_t \tag{3}$$

Recall that a class-K function is a function f that is strictly increasing and satisfies $f(0) = 0$. A function $f : \mathbb{R}^n \to \mathbb{R}$ is locally Lipschitz if, for every $x_0 \in \mathbb{R}^n$, there exists a neighborhood U of x_0 and $L > 0$ such that $|f(x) - f(y)| \leq L||x - y||_2$ for all $x, y \in U$.

IV. Stochastic CBF under Complete Information

This section presents our construction of control barrier functions (CBFs) for stochastic systems where the controller has complete state information. We first present the problem statement and then our barrier function construction and proof.

A. Problem Statement

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

$$dx_t = (f(x_t) + g(x_t)u_t)\ dt + \sigma(x_t)dW_t \tag{4}$$

where $f : \mathbb{R}^n \to \mathbb{R}^n$, $g : \mathbb{R}^n \times \mathbb{R}^{n\times m}$, and $\sigma : \mathbb{R}^n \to \mathbb{R}^n$ are locally Lipschitz continuous functions and W_t is a Brownian motion. We assume that (4) has a strong solution.

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 specified safe operating region. The set $\mathcal{C}$ is defined by a locally Lipschitz function $h : \mathbb{R}^n \to \mathbb{R}$ as

$$\mathcal{C} = \{\mathbf{x} : h(\mathbf{x}) \geq 0\}$$
$$\delta\mathcal{C} = \{\mathbf{x} : h(\mathbf{x}) = 0\}$$

consistent with [8], [9]. The problem statement is, *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 maximal probability?*

B. Control Barrier Function Construction

Our construction of a stochastic control barrier function is given as follows.

Definition 5: Let x_t be a stochastic process described by an equation of the form (2). A control barrier function $B : \mathbb{R}^n \to \mathbb{R}$ is locally Lipschitz and twice-differentiable on int($\mathcal{C}$) and satisfies the following properties:

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

$$\frac{1}{\alpha_1(h(x))} \leq B(x) \leq \frac{1}{\alpha_2(h(x))} \tag{5}$$

for all x.

2) There exists a class-K function α_3 such that

$$\frac{\partial B}{\partial x}a(x) + \mathbf{tr}\left(\frac{1}{2}\sigma(x)^T\frac{\partial^2 B}{\partial x^2}\sigma(x)\right) \leq \alpha_3(h(x)) \tag{6}$$

In the deterministic case, the construction of the CBF $B(x)$ ensures that $B(x) \sim \frac{1}{h(x)}$, and hence that $B(x)$ tends to infinity as the system state approaches the boundary of the safe region $\mathcal{C}$. Consequently, by selecting a controller that ensures that $B(x)$ remains finite (6), the safety of the system is guaranteed. 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. This fact is made explicit by the following theorem.

Theorem 1: Suppose that there exists a CBF for a process x_t described by (2). Then for all t, $Pr(x_t \in \mathcal{C}) = 1$, provided that $\mathbf{x}_0 \in \mathcal{C}$.

Proof: Let B be a CBF and define $B_t = B(x_t)$. Since each sample path of x_t is continuous, each sample path of B_t is continuous. Hence, if $x_t \notin \mathcal{C}$ for some t, then there exists $t' < t$ such that $h(x_{t'}) = 0$ and, by Eq. (5), $B_{t'} = \infty$. As a result, if for all $t > 0$ and $\delta \in (0, 1)$, we have

$$Pr\left(\sup_{t'<t} B_{t'} = \infty\right) < \delta,$$

then $Pr(x_t \in \mathcal{C}) = 1$ for all t.

Let $t > 0$ and $\delta > 0$. We will construct $K > 0$ such that $Pr(\sup_{t'<t} B_{t'} > K) < \delta$. Let $L = B_0$, and choose a real number K such that

$$K > \frac{L + t\alpha_3(\alpha_2^{-1}(\frac{1}{L}))}{\delta}.$$

Define stopping time β as $\beta = \inf\{t : x_t = 2K\}$. We have that $x_{t\wedge\beta}$ is a semimartingale and the function $B(x)$ is twice differentiable on int($\mathcal{C}$), and therefore for any x in a sample path of $x_{t\wedge\beta}$. Hence we can apply Ito's Lemma to obtain

$$\begin{aligned} &B_{t\wedge\beta} \\ &= B_0 + \int_0^{t\wedge\beta} \frac{\partial B}{\partial x}a(x_\tau) + \frac{1}{2}\mathbf{tr}\left(\sigma(x_\tau)^T\frac{\partial^2 B}{\partial x^2}\sigma(x_\tau)\right)\ d\tau \\ &\qquad + \int_0^{t\wedge\beta} \frac{\partial B}{\partial x}\sigma(x_\tau)\ dW_\tau \end{aligned} \tag{7}$$

with probability 1. We construct a sequence of stopping times η_i and ζ_i as

$$\eta_0 = 0, \zeta_0 = \inf\{t : B_t < L\} \tag{8}$$
$$\eta_i = \inf\{t : B_t > L, t > \zeta_{i-1}\},\ i = 1, 2, \ldots, \tag{9}$$
$$\zeta_i = \inf\{t : B_t < L, t > \eta_i\},\ i = 1, 2, \ldots, \tag{10}$$

The times η_i and ζ_i are the up- and down-crossings of B_t over L. Define a random process $\tilde{B}_t$ by

$$\begin{aligned} \tilde{B}_t = L + \sum_{i=0}^{\infty}\Bigg[&\int_{\eta_i\wedge t}^{\zeta_i\wedge t} \alpha_3(\alpha_2^{-1}(\frac{1}{L}))\ d\tau \\ &+ \int_{\eta_i\wedge t}^{\zeta_i\wedge t} \frac{\partial B}{\partial x}\sigma(x_\tau)\ d\tau\Bigg] \end{aligned}$$

We aim to show that, for any sample path where (7) holds, we have $B_{t\wedge\beta} \leq \tilde{B}_{t\wedge\beta}$, or equivalently, $B_{t\wedge\beta} \leq \tilde{B}_{t\wedge\beta}$ with probability 1. The proof is by induction. At $t = 0$, $B_0 = \tilde{B}_0 = L$. For $t \in (\eta_i, \zeta_i]$,

$$\begin{aligned} B_t = B_{\eta_i} &+ \int_{\eta_i}^{t} \frac{\partial B}{\partial x}a(x_\tau) + \frac{1}{2}\mathbf{tr}\left(\sigma(x_\tau)^T\frac{\partial^2 B}{\partial x^2}\sigma(x_\tau)\right)\ d\tau \\ &+ \int_{\eta_i}^{t} \frac{\partial B}{\partial x}\sigma(x_\tau)\ dW_\tau \end{aligned} \tag{11}$$

$$\tilde{B}_t = \tilde{B}_{\eta_i} + \int_{\eta_i}^{t} \alpha_3(\alpha_2^{-1}(\frac{1}{L}))\ d\tau + \int_{\eta_i}^{t} \frac{\partial B}{\partial x}\sigma(x_\tau)\ dW_\tau \tag{12}$$

By induction, $B_{\eta_i} \leq \tilde{B}_{\eta_i}$. The third terms of (11) and (12) are equal. It remains to show that the second term of (11) is a lower bound on the second term of (12). By definition of η_i, $B_\tau \geq L$ for all $\tau \in [\eta, t]$, or equivalently, $\frac{1}{B_\tau} \leq \frac{1}{L}$. By Eq. (5), $B_\tau \leq \frac{1}{\alpha_2(h(x_\tau))}$, and hence $\alpha_2(h(x_\tau)) \leq \frac{1}{B_\tau}$ and $h(x_\tau) \leq \alpha_2^{-1}(\frac{1}{B_\tau})$. We therefore have $h(x_\tau) \leq \alpha_2^{-1}(\frac{1}{B_\tau})$ and $\alpha_3(h(x_\tau)) \leq \alpha_3(\alpha_2^{-1}(\frac{1}{B_\tau}))$. Combining these inequalities with (6) yields

$$\frac{\partial B}{\partial x} a(x_\tau) + \frac{1}{2}\mathbf{tr}\left(\sigma(x_\tau)^T \frac{\partial^2 B}{\partial x^2}\sigma(x_\tau)\right) \leq \alpha_3\left(\alpha_2^{-1}\left(\frac{1}{L}\right)\right),$$

and thus the integrand of the second term of (11) is a lower bound on the integrand of the second term of (12). In particular, $L = B_{\zeta_i} \leq \tilde{B}_{\zeta_i}$.

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

$$\begin{aligned}\tilde{B}_t &= L + \sum_{j=0}^{i}\left[\int_{\eta_j}^{\zeta_j} \alpha_3(\alpha_2^{-1}(\frac{1}{L}))\ d\tau + \int_{\eta_j}^{\zeta_j} \frac{\partial B}{\partial x}\sigma(x_\tau)\ dW_\tau\right] \\ &= \tilde{B}_{\zeta_i} \geq L \geq B_t\end{aligned}$$

by definition of η_i and ζ_i. Hence $B_t \leq \tilde{B}_t$ for all t almost surely. As a corollary, $\tilde{B}_{t\wedge\beta} \geq B_{t\wedge\beta}$ almost surely, and we have

$$\begin{aligned}Pr\left(\sup_{t'\in[0,t]} B_{t'} > K\right) &= Pr\left(\sup_{t'\in[0,t]} B_{t'\wedge\beta} > K\right) \\ &\leq Pr\left(\sup_{t'\in[0,t]} \tilde{B}_{t'\wedge\beta} > K\right)\end{aligned}$$

It therefore suffices to prove that $Pr(\sup_{t'<t} \tilde{B}_{t'\wedge\beta} > K) < \delta$. We first show that $\tilde{B}_t$ is a submartingale. We have

$$\begin{aligned}\mathbf{E}(\tilde{B}_t|\tilde{B}_s) &= \tilde{B}_s + \mathbf{E}\left[\sum_{i=0}^{\infty}\int_{\eta_i\wedge t}^{\zeta_i\wedge t} \alpha_3(\alpha_2^{-1}(\frac{1}{L}))\ d\tau \right. \\ &\quad \left. + \int_{\eta_i\wedge t}^{\zeta_i\wedge t} \frac{\partial B}{\partial x}\sigma(x_\tau)\ dW_\tau\right] \\ &= \tilde{B}_s + \mathbf{E}\left[\sum_{i=0}^{\infty}\int_{\eta_i\wedge t}^{\zeta_i\wedge t} \alpha_3(\alpha_2^{-1}(\frac{1}{L}))\ d\tau\right] \geq \tilde{B}_s\end{aligned}$$

implying that $\tilde{B}_t$ is a submartingale.

Lemma 1 then yields

$$\begin{aligned}KPr\left(\sup_{\tau\in[0,t]} \tilde{B}_{\tau\wedge\beta} > K\right) &\leq \mathbf{E}(\tilde{B}_{t\wedge\beta}) \\ &\leq L + (t\wedge\beta)\alpha_3\left(\alpha_2^{-1}\left(\frac{1}{L}\right)\right) \\ &\leq L + t\alpha_3\left(\alpha_2^{-1}\left(\frac{1}{L}\right)\right).\end{aligned}$$

Rearranging terms and using the choice of K implies that

$$Pr\left(\sup_{\tau\in[0,t]} B_{\tau\wedge\beta} > K\right) \leq \delta,$$

as desired. ■

Theorem 1 implies that, for the SDE (4), the following condition on the controller is sufficient to ensure safety.

Corollary 1: Let $B : \mathbb{R}^n \to \mathbb{R}$ be a twice-differentiable function satisfying (5) for class-K functions α_1 and α_2. Suppose that, at each time t, u_t satisfies

$$\frac{\partial B}{\partial x}(f(x_t)+g(x_t)u_t) + \frac{1}{2}\mathbf{tr}\left(\sigma(x_t)^T\frac{\partial^2 B}{\partial x^2}\sigma(x_t)\right) \leq \alpha_3(h(x)) \tag{13}$$

for some class-K function α_3 and all t. Then the system satisfies $Pr(x_t \in \mathcal{C}) = 1$ for all t

Proof: We show that a function B satisfying the conditions of the corollary is a control barrier function, implying that $Pr(x_t \in \mathcal{C}) = 1$ by Theorem 1. Eq. (5) holds by assumption. Eq. (6) follows from (13), with $a(x) = f(x) + g(x)u$ from Eq. (4). ■

Corollary 1 implies that adding the constraint (13) to the control, which is linear in u_t, is sufficient to ensure safety of the system with probability 1.

Intuitively, almost-sure safety is possible because the controller acts in continuous time with complete information of the system state. Since the system trajectory is continuous, the controller is able to correct for the disturbance at each time t. When only partial or noisy state information is available, however, such safety guarantees may not be possible. This case is discussed in the following section.

V. Stochastic CBF under Incomplete Information

This section considers control barrier functions for stochastic systems with incomplete information due to noisy measurements. We first give the problem statement, and then formulate the stochastic CBF for this case.

A. 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 an output $y_t \in \mathbb{R}^p$ described by the SDEs

$$dx_t = (f(x_t) + g(x_t)u_t)\ dt + \sigma_t\ dV_t \tag{14}$$

$$dy_t = cx_t\ dt + \nu_t\ dW_t \tag{15}$$

where V_t and W_t are Brownian motions, c is a matrix of appropriate dimension, and $f : \mathbb{R}^n \to \mathbb{R}^n$ and $g : \mathbb{R}^n \to \mathbb{R}^{n\times m}$ are locally Lipschitz continuous functions. Define $\overline{f}(x,u) = f(x_t) + g(x_t)u_t$. As a preliminary, the notion of uniform detectability is defined as follows.

Definition 6: The pair $[\frac{\partial\overline{f}}{\partial x}(x,u)\ c]$ is uniformly detectable if there exists a bounded, matrix-valued function $\Lambda(x)$ and a real number $\gamma > 0$ such that

$$w^T\left(\frac{\partial\overline{f}}{\partial x}(x,u) + \Lambda(x)c\right)w \leq -\gamma||w||^2$$

for all w, z, and x.

We make the following additional assumptions on the system dynamics.

Assumption 1: The SDEs (14) and (15) satisfy the following conditions:

1) There exist constants $q, r \in \mathbb{R}_{\geq 0}$ such that $\mathbf{E}(\sigma_t \sigma_t^T) \geq qI$ and $\mathbf{E}(\nu_t \nu_t^T) \geq rI$ for all x and t.
2) The pair $\left[\frac{\partial \overline{f}}{\partial x}(x,u), c\right]$ is uniformly detectable.
3) Let ϕ be defined by

$$\overline{f}(x,u) - \overline{f}(\hat{x},u) = \frac{\partial \overline{f}}{\partial x}(x-\hat{x}) + \phi(x,\hat{x},u)$$

Then there exist real numbers k_ϕ and ϵ_ϕ such that

$$||\phi(x,\hat{x},u)|| \leq k_\phi ||x-\hat{x}||_2^2$$

for all x and $\hat{x}$ satisfying $||x-\hat{x}||_2 \leq \epsilon_\phi$.

The safety condition is defined as in Section IV-A, i.e., the safe region $\mathcal{C}$ is given by $\mathcal{C} = \{x : h(x) \geq 0\}$, with boundary $\delta C = \{x : h(x) = 0\}$, where h is a locally Lipschitz function.

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 $(1-\epsilon)$?

B. Solution Approach

Our solution approach is in two parts. First, we consider 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, enabling application of the approach derived in Section IV.

For the state estimation, we use the Extended Kalman Filter (EKF) [21], which we select due to its widespread applicability (including lightweight embedded implementations) and availability of provable error bounds. The estimated state is equal to $\hat{x}_t$. Define matrix A_t by

$$A_t = \frac{\partial \overline{f}}{\partial x}(\hat{x}(t), u(t))$$

that is, the linearization of $\overline{f}$ around $(\hat{x}, u)$. The Kalman gain matrix K_t is defined by $K_t = P_t c_t^T R_t^{-1}$, where $R_t = \nu_t \nu_t^T$ is a time-varying positive definite matrix. P_t is the solution to the Riccati differential equation

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

where $Q_t = \sigma_t \sigma_t^T$. The EKF estimator is then defined by the SDE

$$d\hat{x}_t = f(\hat{x}_t, u_t)\ dt + K_t(dy_t - c\hat{x}_t\ dt). \tag{16}$$

The following result describes the estimation accuracy of the EKF.

Proposition 1 ([21]): If the conditions of Assumption 1 hold, then for any $\epsilon > 0$, there exists $\gamma > 0$ such that

$$Pr\left(\sup_{t \geq 0} ||x_t - \hat{x}_t||_2 \leq \gamma\right) \geq 1 - \epsilon. \tag{17}$$

Note that Proposition 1 requires that u is bounded, which is implicit in Assumption 1. Define

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

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

Lemma 3: If $||x_t - \hat{x}_t||_2 \leq \gamma$ for all t and $h(\hat{x}_t) > \overline{h}_\gamma$ for all t, then $x_t \in \mathcal{C}$ for all t.

Proof: Suppose that $x_t \notin \mathcal{C}$ for some t. Since each sample path of x_t is continuous, we must have $h(x_\tau) = 0$ for some $\tau \in [0,t]$. By assumption, $||\hat{x}_\tau - x_\tau||_2 \leq \gamma$, i.e., $\hat{x}_\tau \in B(x_\tau, \gamma)$. Since $x_\tau \in h^{-1}(\{0\})$, we have

$$\begin{aligned} h(\hat{x}_\tau) &\leq \sup\{h(x) : ||x - x_\tau||_2 \leq \gamma\} \\ &\leq \sup\{h(x) : ||x - x^0||_2 \leq \gamma \text{ for some } x^0 \in h^{-1}(\{0\})\} \\ &= \overline{h}_\gamma. \end{aligned}$$

This, however, contradicts the assumption that $h(\hat{x}_\tau) > \overline{h}$, and hence we must have $x_t \in \mathcal{C}$ for all t. ∎

Combining Proposition 1 and Lemma 3, 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 that guarantees $h(\hat{x}_t) > \overline{h}_\gamma$ for all t. Define $\hat{h}(x) = h(x) - \overline{h}_\gamma$.

The following theorem gives a sufficient condition for a controller to satisfy the safety constraint in the partial information case.

Theorem 2: Suppose that there exists a function $B : \mathbb{R}^n \to \mathbb{R}$ and class-K functions α_1, α_2, and α_3 such that

$$\frac{1}{\alpha_1(\hat{h}(x))} \leq B(x) \leq \frac{1}{\alpha_2(\hat{h}(x))} \tag{18}$$

$$\begin{aligned} \frac{\partial B}{\partial x}\left(\overline{f}(\hat{x}_t, u_t) + \gamma ||\frac{\partial B}{\partial x} K_t c||_2\right) + \frac{1}{2}\mathbf{tr}\left(\nu_t^T K_t^T \frac{\partial^2 B}{\partial x^2} K_t \nu_t\right) \\ \leq \alpha_3(\hat{h}(\hat{x}_t)) \end{aligned} \tag{19}$$

and γ satisfies (17) for some $\epsilon > 0$. Then $Pr(x_t \in \mathcal{C}\ \forall t) \geq (1-\epsilon)$.

Proof: Our approach is to show that $\hat{h}(\hat{x}_t) \geq 0$ for all t if $||x_t - \hat{x}_t||_2 \leq \gamma$. Combining Eqs. (15) and (16), we have

$$\begin{aligned} d\hat{x}_t &= \overline{f}(\hat{x}_t, u_t)\ dt + K_t(cx_t\ dt + \nu_t dW_t - c\hat{x}_t\ dt) \\ &= (\overline{f}(\hat{x}_t, u_t) + K_t c(x_t - \hat{x}_t))\ dt + K_t \nu_t\ dW_t \end{aligned}$$

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

$$\begin{aligned} dB_t = \Bigg(\frac{\partial B}{\partial x}\left(\overline{f}(\hat{x}_t, u_t) + K_t c(x_t - \hat{x}_t)\right) \\ + \frac{1}{2}\mathbf{tr}\left(\nu_t^T K_t^T \frac{\partial^2 B}{\partial x^2} K_t \nu_t\right)\Bigg)\ dt + \frac{\partial B}{\partial x} K_t \nu_t dW_t \end{aligned} \tag{20}$$

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

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

Hence, if (19) holds, then

$$\begin{aligned} &\frac{\partial B}{\partial x}\left(\overline{f}(\hat{x}_t, u_t) + K_t c(x_t - \hat{x}_t)\right) + \frac{1}{2}\mathbf{tr}\left(\nu_t^T K_t^T \frac{\partial^2 B}{\partial x^2} K_t \nu_t\right) \\ &\leq \frac{\partial B}{\partial x}\left(\overline{f}(\hat{x}_t, u_t) + \gamma ||\frac{\partial B}{\partial x} K_t c||_2\right) \\ &\quad + \frac{1}{2}\mathbf{tr}\left(\nu_t^T K_t^T \frac{\partial^2 B}{\partial x^2} K_t \nu_t\right) \leq \alpha_3(\hat{h}(\hat{x}_t)) \end{aligned}$$

and thus $Pr(\hat{h}(\hat{x}_t) \geq 0\ \forall t) = 1$ by Theorem 1. ∎

Theorem 2 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 instant such that (19) 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.

We note that the condition (18) does not depend on the variance of the process noise. The process noise nonetheless affects the performance of our approach because of its impact on the estimation error $(x_t - \hat{x}_t)$.

In the special case where the system dynamics are linear, the EKF is the minimum mean-square estimator, and the following error bound holds.

Lemma 4: Suppose that $f(x_t) = Ax_t$ and $g(x_t) = B$ where A and B are known, constant matrices. Let $\lambda^* = \sup_t \lambda_{max}(P_t)$, where $\lambda_{max}(\cdot)$ denotes maximum eigenvalue. Let $\gamma = \sqrt{\frac{n\lambda^*}{\epsilon}}$. If u_t is chosen such that (18) and (19) hold, then $Pr(x_t \in \mathcal{C}\ \forall t) \geq (1-\epsilon)$.

Proof: By Theorem 2, it suffices to show that $Pr\left(\sup_t ||x_t - \hat{x}_t||_2 \geq \gamma\right) \leq \epsilon$. We have that

$$\begin{aligned} &Pr\left(\sup_t ||x_t - \hat{x}_t||_2 \geq \gamma\right) \\ &= Pr\left(\sup_t (x_t - \hat{x}_t)^T (x_t - \hat{x}_t) \geq \gamma^2\right) \\ &= Pr\left(\sup_t (x_t - \hat{x}_t)^T \frac{1}{\lambda^*}(x_t - \hat{x}_t) \geq \frac{\gamma^2}{\lambda^*}\right) \end{aligned}$$

By definition, $\frac{1}{\lambda^*} I \leq P_t^{-1}$ for all t, and hence we have

$$\begin{aligned} &Pr\left(\sup_t (x_t - \hat{x}_t)^T \frac{1}{\lambda^*}(x_t - \hat{x}_t) \geq \frac{\gamma^2}{\lambda^*}\right) \\ &\qquad \leq Pr\left(\sup_t (x_t - \hat{x}_t)^T P_t^{-1}(x_t - \hat{x}_t) \geq \frac{\gamma^2}{\lambda^*}\right) \end{aligned}$$

The random process $V_t = (x_t - \hat{x}_t)^T P_t^{-1}(x_t - \hat{x}_t)$ is a submartingale [21], [22], and hence we can apply Doob's martingale inequality to obtain

$$\begin{aligned} &Pr\left(\sup_t (x_t - \hat{x}_t)^T P_t^{-1}(x_t - \hat{x}_t) \geq \frac{\gamma^2}{\lambda^*}\right) \\ &\leq \left(\frac{\gamma^2}{\lambda^*}\right)^{-1} \lim_{t\to\infty} \mathbf{E}\left((x_t - \hat{x}_t)^T P_t^{-1}(x_t - \hat{x}_t)\right) \\ &= n\left(\frac{\lambda^*}{\gamma^2}\right) = \epsilon, \end{aligned}$$

as desired. ∎

An additional challenge is computing the threshold $\overline{h}$. This computation will depend on the choice of h. When h is of the form $h(x) = a^T x - b$, for example, the value of $\overline{h}$ can be obtained as the value of the quadratic program

$$\begin{array}{ll} \text{maximize} & a^T x - b \\ x, x_0 & \\ \text{s.t.} & (x - x_0)^2 \leq \gamma^2 \\ & a^T x_0 = b \end{array} \tag{21}$$

VI. Control Policies from CBFs

This section discusses how control policies be synthesized using control barrier functions. We consider a case where the goal of the system is to minimize the expected value of a quadratic objective function

$$V_t(x_t, u_t) = \begin{pmatrix} x_t^T & u_t^T \end{pmatrix} \begin{pmatrix} Q_t & S_t \\ S_t^T & R_t \end{pmatrix} \begin{pmatrix} x_t \\ u_t \end{pmatrix}.$$

The objective function may arise as a quadratic approximation to the value function of an optimal control problem. In the complete information case, the controller input u_t at time t is equal to the solution of

$$\begin{array}{ll} \text{minimize} & V_t(x_t, u_t) \\ u_t & \\ \text{s.t.} & \frac{\partial B}{\partial x} f(x_t) + \frac{\partial B}{\partial x} g(x_t) u_t + \frac{1}{2}\mathbf{tr}\left(\sigma(x_t)^T \frac{\partial^2 B}{\partial x^2}\sigma(x_t)\right) \\ & \leq \alpha_3(h(x_t)) \end{array} \tag{22}$$

where B is the chosen CBF. Eq. (22) is a quadratic program, which can be solved efficiently using embedded processors.

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

$$\begin{array}{ll} \text{minimize} & V_t(\hat{x}_t, u_t) \\ u_t & \\ \text{s.t.} & \frac{\partial B}{\partial x}\left(f(\hat{x}_t) + g(\hat{x}_t)u_t + \gamma||\frac{\partial B}{\partial x} K_t c||_2\right) \\ & + \frac{1}{2}\mathbf{tr}\left(\nu_t^T K_t^T \frac{\partial^2 B}{\partial x^2} K_t \nu_t\right) \leq \alpha_3(h(\hat{x}_t) - \overline{h}) \\ & ||u_t|| \leq Z \end{array} \tag{23}$$

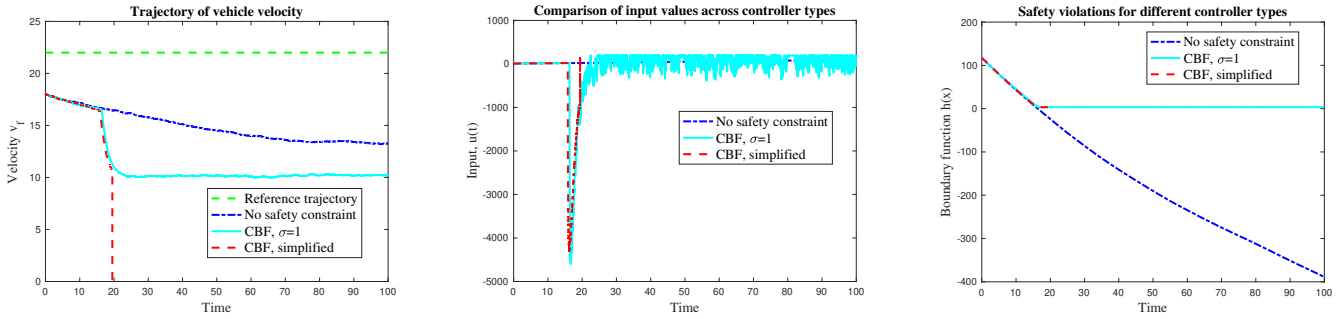
where Z is an upper bound on u_t chosen to ensure that Assumption 1 is satisfied. Eq. (23) is also a quadratic program. We further observe that the program can be extended to describe multiple safety constraints, for example, when the region $\mathcal{C} = \bigcap_{i=1}^N \{x : h_i(x) \geq 0\}$. This extension can be performed by having a set of linear constraints, one for each constraint $\{h_i(x) \geq 0\}$. There is no guarantee, however, that such a program has a feasible solution u_t.

The remaining design specification is the choice of barrier function $B(x)$. One applicable function considered in [9] is $B(x) = \frac{1}{h(x)}$. By inspection, $B(x)$ satisfies the conditions of Definition 5 with $\alpha_1(y) = \alpha_2(y) = y$. For this function, the partial derivatives and Jacobian matrix are given by

$$\begin{aligned} \frac{\partial h}{\partial x_i} &= -\frac{h_{x_i}(x)}{h(x)^2} \\ \frac{\partial^2 h}{\partial x_i \partial x_j} &= -\left(\frac{h_{x_i x_j}(x)h(x) - 2h_{x_i}(x)h_{x_j}(x)h(x)}{h(x)^4}\right) \end{aligned}$$

which can be readily computed when the first and second derivatives of h are known. For example, when $h(x) = a^T x - b$, we have

$$\begin{aligned} \frac{\partial h}{\partial x_i} &= -\frac{a_i}{(a^T x - b)^2} \\ \frac{\partial^2 B}{\partial x_i \partial x_j} &= \frac{2}{(a^T x - b)^3} a a^T \end{aligned}$$



(a) (b) (c)

Fig. 1: Numerical evaluation of our approach using an automatic cruise control example. The goal of the vehicle is to maintain a desired velocity while minimizing control effort and avoiding collisions with the leading vehicle. We simulated a naive controller that does not incorporate safety constraints, our proposed CBF approach, and a simplified CBF approach that treats the EKF estimates as true state values. (a) Velocity trajectories under each approach. The velocity of the leading vehicle is below the desired reference value, and hence the two CBF-based controllers slow down to avoid collisions while the naive controller attempts to track the reference velocity. (b) Control input over time. Both CBF approaches rapidly brake in order to avoid collision, and otherwise have similar input magnitudes to the naive approach. (c) Safety violations. Both the naive and simplified CBF controllers violate safety constraints, while our proposed approach satisfies the safety constraints.

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

Proposition 2 ([23]): Suppose that there exists a function $V : \mathbb{R}^n \to \mathbb{R}$ such that

$$\frac{\partial V}{\partial x}(f(x) + g(x)u) + \mathbf{tr}(\sigma^T \frac{\partial^2 V}{\partial x^2}\sigma) \leq 0 \qquad (24)$$

for all x. Then 0 is stochastically asymptotically stable.

Eq. (24) implies that stability requirements can be incorporated as a linear constraint on the optimization-based control.

VII. Numerical Study

Our proposed approach was validated through a numerical study using a modified version of the automatic cruise control example introduced in [9]. We consider a system with three states $(x_1\ x_2\ x_3)^T$, where $x_1 = v_f$ denotes the velocity of the following vehicle, x_2 denotes the velocity of the leading vehicle, and x_3 denotes the distance between the vehicles. The velocity of the leading vehicle was chosen as a constant. The input is the force applied to the following vehicle, leading to dynamics

$$dx_t = \begin{pmatrix} -F_r(x_t)/M \\ 0 \\ x_2 - x_1 \end{pmatrix} + \begin{pmatrix} 1/M \\ 0 \\ 0 \end{pmatrix} u + dW_t \qquad (25)$$

where $F_r(x) = f_0 + f_1 v_f + f_2 v_f^2$ is the aerodynamic drag with constants $f_0 = 0.1$, $f_1 = 5$, and $f_2 = 0.25$. The mass $M = 1650$. The initial state was chosen as $x_1 = 18$, $x_2 = 10$, and $x_3 = 150$. W_t is a Brownian motion.

The goal of the following vehicle is to achieve a desired velocity $v_d = 22$ while minimizing control effort (defined as the integral of u_t^2) and avoiding collision with the lead vehicle. The collision constraint is encoded as $x_3 - 1.8x_1 \geq 0$, which is linear in x. The target velocity is encoded in a CLF $V(x) = (x_1 - v_d)^2$.

We compared three controllers for this problem. The first controller is a naive optimization-based controller that, at each time t, minimizes the objective function

$$(u\ \delta)\begin{pmatrix} 1 & 0 \\ 0 & 100 \end{pmatrix}\begin{pmatrix} u \\ \delta \end{pmatrix},$$

under the constraint $\dot{V}(x,u) \leq \delta$. Hence the controller attempts to follow the instruction encoded in the CLF while minimizing the control input magnitude, but does not consider safety. The second controller is our proposed CBF based on the measurement $dy_t = x_t dt + dV_t$, where dV_t is a Brownian motion. The parameter γ in our method was selected by simulating the nonlinear dynamics (25) in the absence of any control, observing the maximum deviation $||x - \hat{x}||_2$ between the estimated and actual value, and choosing γ to be ten times this maximum deviation. The barrier function was chosen as

$$B(x) = -\log\left(\frac{h(x)}{1 + h(x)}\right),$$

and $\alpha_3(x) = 1/x$.

The third controller that we simulated was a simplified version of the CBF method. In this version, the barrier function constraint was equal to

$$\frac{\partial B}{\partial x}(f(\hat{x}_t) + g(\hat{x}_t)u) \leq \alpha_3(B(\hat{x}_t)).$$

This constraint can be interpreted as a deterministic CBF based on the estimated value $\hat{x}_t$.

The results of the simulation are shown as Figure 1. The naive method begins to approximate the desired velocity (Fig. 1(a)), but violates the safety constraint because of the desired velocity exceeds the velocity of the leading vehicle, resulting in a collision (Fig. 1(c)). The CBF method, on

the other hand, tracks the naive method until it begins to approach the lead vehicle, triggering a sudden braking (Fig. 1(b)) in order to avoid collision. The CBF then settles on a slower velocity that matches the leading vehicle, with control input magnitude comparable to the naive case following the initial braking maneuver. The CBF method satisfies the safety constraint for all time t (Fig. 1(c)).

The simplified CBF method also tracks with the naive method and attempts to brake in order to avoid collision, however, the braking does not occur rapidly enough because it fails to incorporate the impact of process and measurement noise (Fig. 1(b)). This results in a safety violation (Fig. 1(c)). This example illustrates that the uncertainty arising due to noise must be incorporated when choosing the control action, and that adopting a "certainty equivalent" control strategy based on an estimator may be insufficient to ensure safety.

VIII. Conclusions and Future Work

This paper investigated control barrier functions for nonlinear stochastic systems. In the CBF framework, the desired safety properties of the system are mapped to finiteness of a given barrier function that grows as the system approaches the boundary of the safe region. We considered two cases, namely complete information (when the full state information is available) and incomplete information (when only noisy measurements are available). In the complete information case, we derived sufficient conditions based on CBFs for almost sure safety of the system. In the incomplete information case, we proved that the safety of the system can be guaranteed if the error between an estimated state and the true state remains bounded by a given parameter. We characterized the probability of safety over an infinite time horizon as a function of the estimation error. In both the complete and information cases, our sufficient conditions can be mapped to linear constraints on the control input at each time, enabling us to design efficient controllers with guarantees on performance, safety, and stability. Our framework was evaluated via numerical study. In future work, we plan to consider systems where the output is a nonlinear function of the state, as well as CBFs for distributed, multi-agent systems.

References

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

[2] S. Prajna, A. Jadbabaie, and G. J. Pappas, "A framework for worst-case and stochastic safety verification using barrier certificates," *IEEE Transactions on Automatic Control*, vol. 52, no. 8, pp. 1415–1428, 2007.

[3] A. Chutinan, "Hybrid system verification using discrete model approximations," *Ph. D. dissertation, Department of Electrical and Computer Engineering, Carnegie Mellon University*, 1999.

[4] S. Ratschan and Z. She, "Safety verification of hybrid systems by constraint propagation based abstraction refinement," in *International Workshop on Hybrid Systems: Computation and Control*. Springer, 2005, pp. 573–589.

[5] S. Mitra, T. Wongpiromsarn, and R. M. Murray, "Verifying cyber-physical interactions in safety-critical systems," *IEEE Security & Privacy*, vol. 11, no. 4, pp. 28–37, 2013.

[6] A. Girard, C. Le Guernic, and O. Maler, "Efficient computation of reachable sets of linear time-invariant systems with inputs," in *International Workshop on Hybrid Systems: Computation and Control*. Springer, 2006, pp. 257–271.

[7] M. Althoff, C. Le Guernic, and B. H. Krogh, "Reachable set computation for uncertain time-varying linear systems," in *Proceedings of the 14th international conference on Hybrid systems: computation and control*. ACM, 2011, pp. 93–102.

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

[9] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs for safety critical systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 8, pp. 3861–3876, 2017.

[10] S.-C. Hsu, X. Xu, and A. D. Ames, "Control barrier function based quadratic programs with application to bipedal robotic walking," in *American Control Conference (ACC), 2015*. IEEE, 2015, pp. 4542–4548.

[11] L. Wang, A. D. Ames, and M. Egerstedt, "Multi-objective compositions for collision-free connectivity maintenance in teams of mobile robots," in *Decision and Control (CDC), 2016 IEEE 55th Conference on*. IEEE, 2016, pp. 2659–2664.

[12] E. Dolginova and N. Lynch, "Safety verification for automated platoon maneuvers: A case study," in *International Workshop on Hybrid and Real-Time Systems*. Springer, 1997, pp. 154–170.

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

[14] C. Tomlin, G. J. Pappas, and S. Sastry, "Conflict resolution for air traffic management: A study in multiagent hybrid systems," *IEEE Transactions on automatic control*, vol. 43, no. 4, pp. 509–521, 1998.

[15] L. Lindemann and D. V. Dimarogonas, "Control barrier functions for signal temporal logic tasks," *IEEE Control Systems Letters*, vol. 3, no. 1, pp. 96–101, 2019.

[16] M. Z. Romdlony and B. Jayawardhana, "Stabilization with guaranteed safety using control lyapunov–barrier function," *Automatica*, vol. 66, pp. 39–47, 2016.

[17] Q. Nguyen and K. Sreenath, "Exponential control barrier functions for enforcing high relative-degree safety-critical constraints," in *American Control Conference (ACC), 2016*. IEEE, 2016, pp. 322–328.

[18] M. Rauscher, M. Kimmel, and S. Hirche, "Constrained robot control using control barrier functions," in *Intelligent Robots and Systems (IROS), 2016 IEEE/RSJ International Conference on*. IEEE, 2016, pp. 279–285.

[19] M. Jankovic, "Control barrier functions for constrained control of linear systems with input delay," in *2018 Annual American Control Conference (ACC)*. IEEE, 2018, pp. 3316–3321.

[20] I. Karatzas and S. Shreve, *Brownian motion and stochastic calculus*. Springer Science & Business Media, 2012, vol. 113.

[21] K. Reif, S. Gunther, E. Yaz, and R. Unbehauen, "Stochastic stability of the continuous-time extended kalman filter," *IEE Proceedings-Control Theory and Applications*, vol. 147, no. 1, pp. 45–52, 2000.

[22] R. E. Kalman, "New methods in wiener filtering theory," in *Proceedings of the First Symposium on Engineering Applications of Random Function Theory and Probability, edited by JL Bogdanoff and F. Kozin, John Wiley & Sons, New York*, 1963.

[23] P. Florchinger, "Feedback stabilization of affine in the control stochastic differential systems by the control lyapunov function method," *SIAM Journal on Control and optimization*, vol. 35, no. 2, pp. 500–511, 1997.