

COMPOSITIONAL CONSTRUCTION OF SAFETY CONTROLLERS FOR NETWORKS OF CONTINUOUS-SPACE POMDPS

NILOOFAR JAHANSHAHI¹, ABOLFAZL LAVAEI², AND MAJID ZAMANI^{3,1}

ABSTRACT. In this paper, we propose a compositional framework for the synthesis of safety controllers for networks of partially-observed discrete-time stochastic control systems (a.k.a. continuous-space POMDPs). Given an estimator, we utilize a discretization-free approach to synthesize controllers ensuring safety specifications over finite-time horizons. The proposed framework is based on a notion of so-called *local control barrier functions* computed for subsystems in two different ways. In the first scheme, no prior knowledge of estimation accuracy is needed. The second framework utilizes a probability bound on the estimation accuracy using a notion of so called *stochastic simulation functions*. In both proposed schemes, we drive sufficient small-gain type conditions in order to compositionally construct control barrier functions for interconnected POMDPs using local barrier functions computed for subsystems. Leveraging compositionality results, the constructed control barrier functions enable us to compute lower bounds on the probabilities that the interconnected POMDPs avoid certain unsafe regions in finite-time horizons. We demonstrate the effectiveness of our proposed approaches by applying them to an adaptive cruise control problem.

1. INTRODUCTION

Large-scale stochastic systems have received significant attentions in the past few years due to their broad applications in modeling many engineering systems such as power grids, road traffic networks and industrial control systems to name a few. Guaranteeing safety and reliability of such complex systems in a formal as well as time- and cost-effective way has always been very challenging. In the past few years, formal verification and synthesis of controllers against safety specifications have gained considerable attentions among both control engineers and computer scientists. In this respect, abstraction-based techniques have been widely employed for the formal synthesis of safety controllers [L⁺96, LSZ20d, TNXJ17]. However, those approaches rely on the state and input set discretization and consequently suffer severely from the *curse of dimensionality*: computational complexity exponentially grows with the dimension of the system. In order to overcome this difficulty, compositional techniques have been introduced in the past few years to construct finite abstractions of interconnected systems based on abstractions of smaller subsystems [SAM17, LSZ19, LSZ20a, NSZ21, LSZ20d, NZ20, LSZ20c, LZ19, LSZ18, LSZ20b, Lav19, LSAZ20].

As another promising alternative, *discretization-free* approaches based on *control barrier functions* have been introduced in the past decade [PJP07, AXGT16, NSZ20a, ACE⁺19, JSZ20, NSZ20c, NSZ20b, ALZ20, ALZ21]. Unfortunately, all above-mentioned literatures on both discretization and discretization-free techniques assume that full state information is available for the sake of controller synthesis which is not the case in many practical applications. Taking this limitation into account, the work in [Cla19] studies a controller synthesis scheme for stochastic systems with incomplete information by assuming a priori knowledge of control barrier functions. Given an estimator with a probabilistic guarantee on the accuracy of estimations, [JJZ20b] studies the controller synthesis problem for partially-observed stochastic systems and proposes a lower bound for the probability of satisfaction of safety specifications over finite-time horizons. A synthesis framework based on control barrier functions for partially-observed jump diffusion systems enforcing complex properties expressed by deterministic finite automata is recently proposed in [JJZ20a] in which a prior knowledge of the estimation accuracy is not required anymore.

The proposed techniques in the above-mentioned literature on partially observed systems assume that control barrier functions have a certain parametric form, such as polynomial, and search for their corresponding coefficients under certain assumptions. Although it may be easy to search for those functions for lower-dimensional systems via existing tools, it is computationally very expensive (if not impossible) to compute them for large-scale interconnected systems. Motivated by this challenge, we propose here a compositional approach for the construction of control barrier functions for partially-observed discrete-time stochastic control systems (a.k.a. POMDPs). To the best of our knowledge, this paper is the first to develop a compositional controller synthesis scheme for networks of POMDPs based on barrier functions. By driving small-gain type conditions, we compositionally construct a control barrier function for the interconnected POMDP based on local barrier functions of subsystems. Accordingly, by leveraging the constructed barrier function and the corresponding controller, we compute a lower bound on the probability that the interconnected POMDP avoids an unsafe region over a finite-time horizon.

Particularly, we propose two distinct approaches for the construction of control barrier functions. In the first one, local control barrier functions are defined over augmented systems consisting of subsystems and their estimators. This formulation makes it possible to search for local control barrier functions, and as a result the overall one, without requiring explicitly the accuracies of estimators in probability. In the second framework, local control barrier functions are constructed using the estimators' dynamics (without augmenting them with the subsystems' dynamics) in where we utilize a notion of so-called *stochastic simulation functions* to compute a probabilistic bound on the estimation accuracy. We propose a sum-of-squares (SOS) optimization approach to search for local control barrier functions in both approaches, and accordingly, to compute the corresponding controllers. In order to illustrate the effectiveness of our proposed results, we apply both approaches to an adaptive cruise control problem.

2. PRELIMINARIES AND PROBLEM DEFINITION

2.1. Preliminaries. A probability space in this work is presented by tuple $(\Omega, \mathcal{F}_\Omega, \mathbb{P}_\Omega)$, where Ω is a sample space, \mathcal{F}_Ω is a sigma-algebra on Ω , and \mathbb{P}_Ω is a probability measure that assigns probabilities to events. Random variables introduced here are measurable functions of the form $X : (\Omega, \mathcal{F}_\Omega) \rightarrow (\mathcal{S}_X, \mathcal{F}_X)$ such that any random variable X induces a probability measure on its space $(\mathcal{S}_X, \mathcal{F}_X)$ as $\text{Prob}\{A\} = \mathbb{P}_\Omega\{X^{-1}(A)\}$ for any $A \in \mathcal{F}_X$. We directly present the probability measure on $(\mathcal{S}_X, \mathcal{F}_X)$ without explicitly mentioning the underlying probability space and the function X itself.

We call the topological space \mathcal{S} as a Borel space if it is homeomorphic to a Borel subset of a Polish space. Euclidean space \mathbb{R}^n , its Borel subsets endowed with a subspace topology, and hybrid spaces are examples of Borel spaces. A Borel sigma-algebra is denoted by $\mathfrak{B}(\mathcal{S})$, where any Borel space \mathcal{S} is assumed to be endowed with it. A map $f : \mathcal{S} \rightarrow Y$ is measurable whenever it is Borel measurable.

2.2. Notation. The sets of nonnegative and positive integers are denoted by $\mathbb{N} := \{0, 1, 2, \dots\}$ and $\mathbb{N}_{\geq 1} := \{1, 2, 3, \dots\}$, respectively. Moreover, symbols $\mathbb{R}, \mathbb{R}_{>0}$, and $\mathbb{R}_{\geq 0}$ denote, respectively, the sets of real, positive and nonnegative real numbers. Given N vectors $x_i \in \mathbb{R}^{n_i}, n_i \in \mathbb{N}_{\geq 1}, i \in \{1, \dots, N\}$, we use $x = [x_1; \dots; x_N]$ to denote the corresponding column vector of the dimension $\sum_i n_i$. We denote by $\|\cdot\|$ the infinity norm. Given any $a \in \mathbb{R}$, $|a|$ denotes the absolute value of a . The identity function and composition of functions are denoted by \mathcal{I}_d and the symbol \circ , respectively. A function $\kappa : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$, is said to be a class \mathcal{K} function if it is continuous, strictly increasing, and $\kappa(0) = 0$. A class \mathcal{K} function $\kappa(\cdot)$ is said to be a class \mathcal{K}_∞ if $\kappa(r) \rightarrow \infty$ as $r \rightarrow \infty$. We denote the empty set by \emptyset . Given functions $f_i : X_i \rightarrow Y_i$, for any $i \in \{1, \dots, N\}$, their Cartesian product $\prod_{i=1}^N f_i : \prod_{i=1}^N X_i \rightarrow \prod_{i=1}^N Y_i$ is defined as $(\prod_{i=1}^N f_i)(x_1, \dots, x_N) = [f_1(x_1); \dots; f_N(x_N)]$.

2.3. Partially-Observed Discrete-Time Stochastic Control Systems (a.k.a. Continuous-Space POMDPs). In this paper, we consider partially-observed discrete-time stochastic control systems as formalized in the following definition.

Definition 2.1. A partially-observed discrete-time stochastic control system (PO-dt-SCS) in this paper is characterized by the tuple

$$\Sigma = (X, U, W, \varsigma_1, f, Y_1, Y_2, h_1, h_2, \varsigma_2), \quad (2.1)$$

where,

- $X \subseteq \mathbb{R}^n$ is a Borel space as the state space of the system. The measurable space with $\mathfrak{B}(X)$ being the Borel sigma-algebra on the state space is denoted by $(X, \mathfrak{B}(X))$;
- $U \subseteq \mathbb{R}^m$ is a Borel space as the external input space of the system;
- $W \subseteq \mathbb{R}^p$ is a Borel space as the internal input space of the system;
- ς_i , $i \in \{1, 2\}$, denote sequences of independent and identically distributed (i.i.d.) random variables from a sample space Ω to the set $\mathcal{V}_{\varsigma_i}$,

$$\varsigma_i = \{\varsigma_i(k) : \Omega \rightarrow \mathcal{V}_{\varsigma_i}, k \in \mathbb{N}\},$$

- $f : X \times U \times W \times \mathcal{V}_{\varsigma_1} \rightarrow X$ is a measurable function characterizing the state evolution of the system;
- $Y_1 \subseteq \mathbb{R}^p$ is a Borel space as the internal output space of the system;
- $Y_2 \subseteq \mathbb{R}^q$ is a Borel space as the external output space of the system;
- $h_1 : X \rightarrow Y_1$ is a measurable function that maps a state $x \in X$ to its internal output $y_1 = h_1(x)$;
- $h_2 : X \times \mathcal{V}_{\varsigma_2} \rightarrow Y_2$ is a measurable function that maps a state $x(k) \in X$ to its external output $y_2(k) = h_2(x(k), \varsigma_2(k))$.

An evolution of the state of PO-dt-SCS Σ for a given initial state $x(0) \in X$ and input sequences $v(\cdot) : \mathbb{N} \rightarrow U$ and $w(\cdot) : \mathbb{N} \rightarrow W$ is described by

$$\Sigma : \begin{cases} x(k+1) = f(x(k), v(k), w(k), \varsigma_1(k)), \\ y_1(k) = h_1(x(k)), \\ y_2(k) = h_2(x(k), \varsigma_2(k)), \end{cases} \quad k \in \mathbb{N}. \quad (2.2)$$

A PO-dt-SCS Σ in (2.1) can be *equivalently* represented as a partially-observed Markov decision process (POMDP) [Kal97, Proposition 7.6]

$$\Sigma = (X, U, W, T_x, Y_1, Y_2, h_1, h_2, \varsigma_2), \quad (2.3)$$

where the map $T_x : \mathfrak{B}(X) \times X \times U \times W \rightarrow [0, 1]$ is a conditional stochastic kernel that assigns to any $x(k) \in X$, $v(k) \in U$, and $w(k) \in W$, a probability measure $T_x(\cdot \mid x(k), v(k), w(k))$ on the measurable space $(X, \mathfrak{B}(X))$ so that for any set $\mathcal{A} \in \mathfrak{B}(X)$,

$$\mathbb{P}(x(k+1) \in \mathcal{A} \mid x(k), v(k), w(k)) = \int_{\mathcal{A}} T_x(x(k+1) \mid x(k), v(k), w(k)).$$

For given inputs $v(\cdot)$, and $w(\cdot)$, the stochastic kernel T_x captures the evolution of the state of Σ and can be uniquely determined by the pair (ς_1, f) from (2.1). Since two systems (2.1) and (2.3) are indeed equivalent, we interchangeably employ terms PO-dt-SCS and POMDP in the remainder of the paper. We associate to U and W sets \mathcal{U} and \mathcal{W} , respectively, to be collections of sequences $\{v(k) : \Omega \rightarrow U, k \in \mathbb{N}\}$ and $\{w(k) : \Omega \rightarrow W, k \in \mathbb{N}\}$, in which $v(k)$ and $w(k)$ are independent of $\varsigma_i(l)$ for any $k, l \in \mathbb{N}$, $l \geq k$ and $i \in \{1, 2\}$. The random sequences $x_{avw} : \Omega \times \mathbb{N} \rightarrow X$, $y_{1avw} : \Omega \times \mathbb{N} \rightarrow Y_1$, and $y_{2avw} : \Omega \times \mathbb{N} \rightarrow Y_2$ satisfying (2.2) are called respectively the *solution process*, *internal output* and *external output processes* of Σ , respectively, under an external input v , an internal input w , and an initial state a .

Since the main goal of this work is to study networks of systems, the tuple representing interconnected systems, not containing internal inputs and outputs, is $\Sigma = (X, U, \varsigma_1, f, Y, h, \varsigma_2)$, where $f : X \times U \times \mathcal{V}_{\varsigma_1} \rightarrow X$, and

$$\Sigma : \begin{cases} x(k+1) = f(x(k), v(k), \varsigma_1(k)), \\ y(k) = h(x(k), \varsigma_2(k)), \end{cases} \quad k \in \mathbb{N}. \quad (2.4)$$

For the sake of controller synthesis using barrier certificates explained later in detail, we raise the following assumption on the existence of an estimator that estimates the state of the PO-dt-SCS in (2.2).

Assumption 1. Consider a PO-dt-SCS $\Sigma = (X, U, W, \varsigma_1, f, Y_1, Y_2, h_1, h_2, \varsigma_2)$. States of Σ in (2.2) can be estimated by a proper estimator $\hat{\Sigma}$ which is characterized by the tuple $\hat{\Sigma} = (X, U, W, \hat{f}, Y_1, Y_2, h_1)$ and represented in the following form:

$$\hat{\Sigma} : \begin{cases} \hat{x}(k+1) = \hat{f}(\hat{x}(k), v(k), \hat{w}(k), y_2(k)), \\ \hat{y}_1(k) = h_1(\hat{x}(k)), \end{cases} \quad (2.5)$$

where v and y_2 are external input and output signals of Σ and \hat{w} is the internal input signal coming from other estimators. We explain later how \hat{w} is being fed by the estimators of other neighbouring subsystems.

There exist numerous results in the relevant literature for the design of the estimator in (2.5) for different classes of stochastic systems (cf. [LWL09, SWL11, WDZH13, SSS09]).

In the next section, we introduce notions of local control barrier functions (LCBF) and control barrier functions (CBF) for respectively POMDPs (with both internal and external inputs) and interconnected POMDPs (without internal inputs and outputs).

3. (LOCAL) CONTROL BARRIER FUNCTIONS

First, we define (local) control barrier functions ((L)CBF) over an augmented system consisting of the stochastic (sub)system's and its estimator's dynamics. This formulation enables one to search for (local) control barrier functions with no prior knowledge of the estimation accuracy. Second, we formulate (local) control barrier functions over the estimator's dynamics (without augmenting them with the subsystem's dynamics) by utilizing a given probability bound on the estimation accuracy computed via a notion of so-called stochastic simulation functions.

3.1. Notions of (L)CBF without considering the estimation accuracy. Here, we first define the augmented process $[x(k); \hat{x}(k)]$, where $x(k)$ and $\hat{x}(k)$ are the solution processes of subsystems Σ in (2.2) and their estimators $\hat{\Sigma}$ in (2.5), respectively. The corresponding augmented stochastic subsystem $\tilde{\Sigma}$ can be defined as:

$$\tilde{\Sigma} : \begin{bmatrix} x(k+1) \\ \hat{x}(k+1) \end{bmatrix} = \begin{bmatrix} f(x(k), v(k), w(k), \varsigma_1(k)) \\ \hat{f}(\hat{x}(k), v(k), \hat{w}(k), y_2(k)) \end{bmatrix}. \quad (3.1)$$

Now, the local control barrier function is defined for system $\tilde{\Sigma}$ in (3.1). This framework allows us to provide one of our main results without any prior knowledge of the probabilistic distance between the actual states and their estimations. We now formally define local control barrier functions constructed over the augmented system $\tilde{\Sigma}$.

Definition 3.1. Consider a POMDP Σ in (2.2), its estimator $\hat{\Sigma}$ in (2.5), and the resulting augmented system $\tilde{\Sigma}$ in (3.1). Let $X_a, X_b \subseteq X$ represent some initial and unsafe regions, respectively. A function $\mathcal{B} : X \times X \rightarrow \mathbb{R}_{\geq 0}$ is called a local control barrier function (LCBF) for $\tilde{\Sigma}$ if there exist constants $\bar{\psi}, \bar{\gamma} \in \mathbb{R}_{\geq 0}$ and $\bar{\lambda} \in \mathbb{R}_{> 0}$, such that

- $\forall (x, \hat{x}) \in X \times X,$

$$\mathcal{B}(x, \hat{x}) \geq \alpha(\| \begin{bmatrix} h_1(x) \\ h_1(\hat{x}) \end{bmatrix} \|^2), \quad (3.2)$$

- $\forall (x, \hat{x}) \in X_a \times X_a,$

$$\mathcal{B}(x, \hat{x}) \leq \bar{\gamma}, \quad (3.3)$$

- $\forall (x, \hat{x}) \in X_b \times X,$

$$\mathcal{B}(x, \hat{x}) \geq \bar{\lambda}, \quad (3.4)$$

- $\forall \hat{x}(k) \in X, \forall \hat{w}(k) \in W, \exists v(k) \in U$, such that $\forall x(k) \in X, \forall w(k) \in W$,

$$\begin{aligned} & \mathbb{E} \left[\mathcal{B}(f(x(k), v(k), w(k), \varsigma_1(k)), \hat{f}(\hat{x}(k), v(k), \hat{w}(k), y_2(k))) \mid x(k), \hat{x}(k), v(k), w(k), \hat{w}(k)) \right] \\ & \leq \max \left\{ \bar{\kappa} \mathcal{B}(x(k), \hat{x}(k)), \rho(\| \begin{bmatrix} w(k) \\ \hat{w}(k) \end{bmatrix} \|^2), \bar{\psi} \right\}, \end{aligned} \quad (3.5)$$

for some $\alpha \in \mathcal{K}_\infty$, $\rho \in \mathcal{K}_\infty \cup \{0\}$ and $0 < \bar{\kappa} < 1$.

Definition 3.1 can also be stated for interconnected systems without internal inputs and outputs by eliminating all the terms related to the internal input w , its estimation \hat{w} , internal output $h_1(x)$, and its estimation $h_1(\hat{x})$ as defined below.

Definition 3.2. Consider an (interconnected) POMDP $\Sigma = (X, U, \varsigma_1, f, Y, h, \varsigma_2)$, its estimator $\hat{\Sigma}$ also without internal inputs and outputs, and the augmented system $\tilde{\Sigma} = [\Sigma; \hat{\Sigma}]$. Let $X_a, X_b \subseteq X$, respectively, represent initial and unsafe regions. A function $\mathcal{B} : X \times X \rightarrow \mathbb{R}_{\geq 0}$ is called a control barrier function (CBF) for $\tilde{\Sigma}$ if there exist constants $\psi, \gamma \in \mathbb{R}_{\geq 0}$ and $\lambda \in \mathbb{R}_{> 0}$ such that $\gamma < \lambda$, and

$$\begin{aligned} & \bullet \forall (x, \hat{x}) \in X_a \times X_a, \\ & \qquad \qquad \qquad \mathcal{B}(x, \hat{x}) \leq \gamma, \end{aligned} \quad (3.6)$$

$$\begin{aligned} & \bullet \forall (x, \hat{x}) \in X_b \times X, \\ & \qquad \qquad \qquad \mathcal{B}(x, \hat{x}) \geq \lambda, \end{aligned} \quad (3.7)$$

- and $\forall \hat{x}(k) \in X, \exists v(k) \in U$, such that $\forall x(k) \in X$,

$$\mathbb{E} \left[\mathcal{B}(f(x(k), v(k), \varsigma_1(k)), \hat{f}(\hat{x}(k), v(k), y(k))) \mid x(k), \hat{x}(k), v(k) \right] \leq \max \{ \kappa \mathcal{B}(x(k), \hat{x}(k)), \psi \}, \quad (3.8)$$

for some $0 < \kappa < 1$.

Remark 3.3. Note that we need the condition $\gamma < \lambda$ (i.e., $X_a \cap X_b = \emptyset$) in order to provide a meaningful probability in Theorem 3.4 later. This requirement is only for the interconnected system and not for subsystems. In particular, LCBFs are mainly utilized for the compositional construction of CBFs over interconnected systems and are not directly employed for ensuring the probability of safety satisfaction. The above definition associates a policy $\eta : X \rightarrow U$ to a CBF, where X here is the state set of the estimator $\hat{\Sigma}$. Definition 3.2 gives such a policy according to the existential quantifier over the input for any estimator's state $\hat{x} \in X$.

The next theorem shows the usefulness of having a CBF to quantify an upper bound on the exit probability (i.e., the probability that the solution process of the interconnected system reaches the unsafe region in a finite-time horizon) of POMDP (without internal inputs and outputs).

Theorem 3.4. Let $\Sigma = (X, U, \varsigma_1, f, Y, h, \varsigma_2)$ be a POMDP (without internal inputs and outputs) and $\hat{\Sigma}$ be its corresponding estimator. Suppose \mathcal{B} is a CBF according to Definition 3.2. Then, the probability that the solution process of Σ starts from any initial states $x(0) = a \in X_a$ and reaches X_b under the control policy η within a time horizon $[0, T_d]$ is formally upper bounded as

$$\mathbb{P} \left[x_{av}(k) \in X_b \text{ for some } k \in [0, T_d] \mid a, v \right] \leq \delta, \quad (3.9)$$

where,

$$\delta := \begin{cases} 1 - (1 - \frac{\gamma}{\lambda})(1 - \frac{\psi}{\lambda})^{T_d}, & \text{if } \lambda \geq \frac{\psi}{\kappa}, \\ \frac{\gamma}{\lambda}(1 - \kappa)^{T_d} + (\frac{\psi}{\kappa\lambda})(1 - (1 - \kappa)^{T_d}), & \text{if } \lambda < \frac{\psi}{\kappa}. \end{cases} \quad (3.10)$$

The proof of Theorem 3.4 is provided in Appendix.

Remark 3.5. Utilizing the augmented system $\tilde{\Sigma}$ as in (3.1) provides us with the results in Theorem 3.4 with no need of knowing the estimation accuracy explicitly. This allows more flexibility in designing the estimator and potentially results in tighter upper bounds.

In the next subsection, we formulate control barrier functions only over the estimators' dynamics by utilizing a probability bound on the estimation accuracy.

3.2. Notions of (L)CBF by considering the estimation accuracy. Given an estimator with a probabilistic guarantee on the accuracy of the estimation, we propose an approach to construct a CBF defined only over the states of the estimator $\hat{\Sigma}$. For a given time horizon T_d , we assume the probabilistic bound on the accuracy of the estimator is given by [RGYU00]:

$$\forall \epsilon > 0, \exists \theta \in (0, 1], \text{ such that } \mathbb{P} \left[\sup_{0 \leq k \leq T_d} \|x_{av}(k) - \hat{x}_{\hat{a}v}(k)\| < \epsilon \mid a, \hat{a}, v \right] \geq 1 - \theta,$$

for any $a, \hat{a} \in X$ and any $v \in \mathcal{U}$. In order to quantify the distance (a.k.a. error) between a system's state and its estimation, we employ notions of so-called stochastic (pseudo)-simulation functions. To do so, we first introduce stochastic pseudo-simulation functions (SPSF) for POMDPs with both internal and external inputs. We then define stochastic simulation functions (SSF) for interconnected POMDPs without internal inputs and outputs.

Definition 3.6. Consider a POMDP Σ in (2.2) and its corresponding estimator $\hat{\Sigma}$ in (2.5). A function $\phi : X \times X \rightarrow \mathbb{R}_{\geq 0}$ is called a stochastic pseudo-simulation function (SPSF) from $\hat{\Sigma}$ to Σ if

$$(i) \quad \forall x \in X, \forall \hat{x} \in X,$$

$$\varepsilon(\|x - \hat{x}\|) \leq \phi(x, \hat{x}),$$

$$(ii) \quad \forall \hat{x}(k) \in X, \forall \hat{w}(k) \in W, \exists v(k) \in U, \text{ such that } \forall x(k) \in X, \forall w(k) \in W,$$

$$\begin{aligned} & \mathbb{E} \left[\phi(f(x(k), v(k), w(k), \varsigma_1(k)), \hat{f}(\hat{x}(k), v(k), \hat{w}(k), y_2(k))) \mid x(k), \hat{x}(k), v(k), w(k), \hat{w}(k)) \right] \\ & \leq \max \{ \bar{\mu} \phi(x(k), \hat{x}(k)), \varrho(\|w(k) - \hat{w}(k)\|), \bar{c} \}, \end{aligned}$$

for some $0 < \bar{\mu} < 1$, $\varepsilon \in \mathcal{K}_\infty$, $\varrho \in \mathcal{K}_\infty \cup \{0\}$, and $\bar{c} \in \mathbb{R}_{\geq 0}$.

Definition 3.6 can also be stated for POMDPs without internal inputs and outputs by eliminating all the terms related to the internal input w and its estimation \hat{w} as defined below.

Definition 3.7. Consider an (interconnected) POMDP $\Sigma = (X, U, \varsigma_1, f, Y, h, \varsigma_2)$ and its estimator $\hat{\Sigma}$. A function $\phi : X \times X \rightarrow \mathbb{R}_{\geq 0}$ is called a stochastic simulation function (SSF) from $\hat{\Sigma}$ to Σ if

$$(i) \quad \forall x \in X, \forall \hat{x} \in X,$$

$$\varepsilon(\|x - \hat{x}\|) \leq \phi(x, \hat{x}),$$

$$(ii) \quad \forall \hat{x}(k) \in X, \exists v(k) \in U, \text{ such that } \forall x(k) \in X,$$

$$\mathbb{E} \left[\phi(f(x(k), v(k), \varsigma_1(k)), \hat{f}(\hat{x}(k), v(k), y(k))) \mid x(k), \hat{x}(k), v(k)) \right] \leq \max \{ \mu \phi(x(k), \hat{x}(k)), c \},$$

for some $0 < \mu < 1$, $\varepsilon \in \mathcal{K}_\infty$, and $c \in \mathbb{R}_{\geq 0}$.

The next theorem shows how an SSF can be employed to obtain the probability bound on the estimation accuracy.

Theorem 3.8. Consider a POMDP Σ in (2.4), its estimator $\hat{\Sigma}$ in (2.5) (without internal inputs and outputs), and $\epsilon > 0$. Suppose ϕ is an SSF from $\hat{\Sigma}$ to Σ . For any $v \in \mathcal{U}$, and for any random variables a and \hat{a} as initial states of Σ and $\hat{\Sigma}$, respectively, the following inequality holds:

$$\mathbb{P} \left[\sup_{0 \leq k \leq T_d} \|x_{av}(k) - \hat{x}_{\hat{a}v}(k)\| \geq \epsilon \mid a, \hat{a}, v \right] \leq \theta,$$

where,

$$\theta := \begin{cases} 1 - (1 - \frac{\Phi(a, \hat{a})}{\varepsilon(\epsilon)})(1 - \frac{c}{\varepsilon(\epsilon)})^{T_d}, & \text{if } \varepsilon(\epsilon) \geq \frac{c}{\mu}, \\ (\frac{\Phi(a, \hat{a})}{\varepsilon(\epsilon)})(1 - \mu)^{T_d} + (\frac{c}{\mu\varepsilon(\epsilon)})(1 - (1 - \mu)^{T_d}), & \text{if } \varepsilon(\epsilon) < \frac{c}{\mu}. \end{cases} \quad (3.11)$$

The proof of Theorem 3.8 is provided in Appendix.

We now propose our second formulation of control barrier functions defined only over the estimators' dynamics as the following.

Definition 3.9. Consider a POMDP Σ as in (2.2), its estimator $\hat{\Sigma}$, and $\epsilon > 0$. Let $X_a, X_b \subseteq X$ denote respectively initial and unsafe sets. Let us define $X_b^\epsilon := \{\hat{x} \in X \mid \exists x \in X_b, \|\hat{x} - x\| \leq \epsilon\}$ (i.e., unsafe set for $\hat{\Sigma}$). A function $\mathcal{B} : X \rightarrow \mathbb{R}_{\geq 0}$ is called a local control barrier function (LCBF) for $\hat{\Sigma}$ if there exist constants $\psi, \bar{\gamma} \in \mathbb{R}_{\geq 0}$ and $\bar{\lambda} \in \mathbb{R}_{> 0}$, such that

- $\forall x \in X,$

$$\mathcal{B}(x) \geq \alpha(\|h_1(x)\|^2), \quad (3.12)$$

- $\forall x \in X_a,$

$$\mathcal{B}(x) \leq \bar{\gamma}, \quad (3.13)$$

- $\forall x \in X_b^\epsilon,$

$$\mathcal{B}(x) \geq \bar{\lambda}, \quad (3.14)$$

- and $\forall \hat{x}(k) \in X, \forall \hat{w}(k) \in W, \exists v(k) \in U,$ such that $\forall y_2(k) \in Y_2,$

$$\mathbb{E}[\mathcal{B}(\hat{f}(\hat{x}(k), v(k), \hat{w}(k), y_2(k))) \mid \hat{x}(k), v(k), \hat{w}(k)] \leq \max\{\bar{\kappa}\mathcal{B}(\hat{x}(k)), \rho(\|\hat{w}(k)\|^2), \bar{\psi}\}, \quad (3.15)$$

for some $0 < \bar{\kappa} < 1$, $\alpha \in \mathcal{K}_\infty$, and $\rho \in \mathcal{K}_\infty \cup \{0\}$.

We now modify Definition 3.9 and present it for the interconnected POMDPs as the following.

Definition 3.10. Consider an (interconnected) POMDP $\Sigma = (X, U, \varsigma_1, f, Y, h, \varsigma_2)$, its estimator $\hat{\Sigma}$ without internal inputs and outputs and $\epsilon > 0$. Let $X_a, X_b \subseteq X$ denote respectively initial and unsafe sets. Let us define $X_b^\epsilon := \{\hat{x} \in X \mid \exists x \in X_b, \|\hat{x} - x\| \leq \epsilon\}$. A function $\mathcal{B} : X \rightarrow \mathbb{R}_{\geq 0}$ is called a control barrier function for $\hat{\Sigma}$ if there exist constants $\psi, \gamma \in \mathbb{R}_{\geq 0}$ and $\lambda \in \mathbb{R}_{> 0}$ such that $\gamma < \lambda$ and

- $\forall x \in X_a,$

$$\mathcal{B}(x) \leq \gamma,$$

- $\forall x \in X_b^\epsilon,$

$$\mathcal{B}(x) \geq \lambda,$$

- and $\forall \hat{x}(k) \in X, \exists v(k) \in U,$ such that $\forall y(k) \in Y,$

$$\mathbb{E}[\mathcal{B}(\hat{f}(\hat{x}(k), v(k), y(k))) \mid \hat{x}(k), v(k)] \leq \max\{\kappa\mathcal{B}(\hat{x}(k)), \psi\},$$

for some $0 < \kappa < 1$.

One can employ Definition 3.10 and provide a similar result as Theorem 3.4:

$$\mathbb{P}[\hat{x}_{\hat{a}v}(k) \in X_b^\epsilon \text{ for some } k \in [0, T_d] \mid \hat{a}, v] \leq \delta,$$

where δ is computed as in (3.10). In the next Theorem, we provide an upper bound on the exit probability of POMDP using the estimation accuracy.

Theorem 3.11. *Let $\Sigma = (X, U, \varsigma_1, f, Y, h, \varsigma_2)$ be a POMDP without internal inputs and outputs, $\hat{\Sigma}$ be its corresponding estimator and ϵ be a positive constant. Suppose \mathcal{B} is a CBF for $\hat{\Sigma}$ as in Definition 3.10. Then, the probability that the solution process of Σ starts from any initial state $x(0) = a \in X_a$ and reaches X_b under control policy η within a time horizon $[0, T_d]$ is upper bounded as*

$$\mathbb{P}[x_{av}(k) \in X_b \text{ for some } k \in [0, T_d] \mid a, v] \leq \delta + \theta, \quad (3.16)$$

where δ and θ are computed as in (3.10) and (3.11), respectively.

The proof is similar to that of [JJZ20a, Theorem 3.3] and is omitted here due to lack of space.

Remark 3.12. *Note that the first proposed approach does not require a prior knowledge of the estimation accuracy, and accordingly, it gives the user more flexibility on the estimator design. Moreover, in the first approach the computation of the exit probability can be done in one shot without utilizing SSFs and, hence, be less conservative. However, the computational complexity in the first approach is more than the second one since the control barrier function should be constructed over the augmented system.*

In the next sections, we analyze networks of POMDP and discuss under which conditions one can construct a CBF of an interconnected system based on LCBF of its subsystems.

4. INTERCONNECTED POMDP

We consider a collection of partially-observed stochastic control subsystems and their estimators as

$$\begin{aligned} \Sigma_i &= (X_i, U_i, W_i, \varsigma_{1i}, f_i, Y_{1i}, Y_{2i}, h_{1i}, h_{2i}, \varsigma_{2i}), \\ \hat{\Sigma}_i &= (X_i, U_i, W_i, \hat{f}_i, Y_{1i}, Y_{2i}, h_{1i}), \quad i \in \{1, \dots, N\}, \end{aligned}$$

where internal inputs and outputs are partitioned as

$$\begin{aligned} w_i &= [w_{i1}; \dots; w_{i(i-1)}; w_{i(i+1)}; \dots; w_{iN}], \\ y_{1i} &= [y_{1i1}; \dots; y_{1i(i-1)}; y_{1i(i+1)}; \dots; y_{1iN}], \end{aligned} \quad (4.1)$$

and their internal output spaces and functions are of the form

$$\begin{aligned} Y_{1i} &= \prod_{j=1, j \neq i}^N Y_{1ij}, \\ h_{1i}(x_i) &= [h_{1i1}(x_i); \dots; h_{1i(i-1)}(x_i); h_{1i(i+1)}(x_i); \dots; h_{1iN}(x_i)]. \end{aligned} \quad (4.2)$$

Furthermore, the internal input and output of the estimators are also partitioned similar to (4.1) and (4.2).

Outputs y_{1ij} with $i \neq j$ are *internal* outputs which are employed for the sake of interconnections. If there is a connection from Σ_j to Σ_i , we assume that w_{ij} is equal to y_{1ji} . Otherwise, the connecting output function is identically zero, i.e., $h_{1ji} \equiv 0$. The same interconnections hold for the estimators. If there is a connection from $\hat{\Sigma}_j$ to $\hat{\Sigma}_i$, we assume that \hat{w}_{ij} is equal to \hat{y}_{1ji} . Otherwise, the connecting output function is identically zero, i.e., $\hat{h}_{1ji} \equiv 0$. Now we define interconnected partially-observed stochastic control systems.

Definition 4.1. *Consider $N \in \mathbb{N}_{\geq 1}$ POMDPs $\Sigma_i = (X_i, U_i, W_i, \varsigma_{1i}, f_i, Y_{1i}, Y_{2i}, h_{1i}, h_{2i}, \varsigma_{2i})$, $i \in \{1, \dots, N\}$, with the input-output configuration as in (4.1)-(4.2). The interconnection of Σ_i , for any $i \in \{1, \dots, N\}$, is the interconnected POMDP $\Sigma = (X, U, \varsigma_1, f, Y, h, \varsigma_2)$, denoted by $\mathcal{I}(\Sigma_1, \dots, \Sigma_N)$, such that $X := \prod_{i=1}^N X_i$, $U := \prod_{i=1}^N U_i$, $\varsigma_1 = [\varsigma_{11}; \dots; \varsigma_{1N}]$, $f := \prod_{i=1}^N f_i$, $Y := \prod_{i=1}^N Y_i$, $h := \prod_{i=1}^N h_i$, and $\varsigma_2 = [\varsigma_{21}; \dots; \varsigma_{2N}]$, subjected to the following constraint:*

$$\forall i, j \in \{1, \dots, N\}, i \neq j : \quad w_{ji} = y_{1ij}, \quad Y_{1ij} \subseteq W_{ji}.$$

In a similar way, we define the interconnection of estimators $\hat{\Sigma}$ as the following.

Definition 4.2. Consider $N \in \mathbb{N}_{\geq 1}$ estimators $\hat{\Sigma}_i = (X_i, U_i, W_i, \hat{f}_i, Y_{1_i}, Y_{2_i}, h_{1_i})$, $i \in \{1, \dots, N\}$, with the input-output configuration similar to (4.1)-(4.2). The interconnection of $\hat{\Sigma}_i$, for any $i \in \{1, \dots, N\}$, is the interconnected estimator $\hat{\Sigma} = (X, U, \hat{f}, Y)$, denoted by $\mathcal{I}(\hat{\Sigma}_1, \dots, \hat{\Sigma}_N)$, such that $X := \prod_{i=1}^N X_i$, $U := \prod_{i=1}^N U_i$, $\hat{f} := \prod_{i=1}^N \hat{f}_i$, and $Y := \prod_{i=1}^N Y_i$, subject to the following constraint:

$$\forall i, j \in \{1, \dots, N\}, i \neq j: \quad \hat{w}_{ji} = \hat{y}_{1_{ij}}, \quad Y_{1_{ij}} \subseteq W_{ji}.$$

An example of the interconnection of two POMDPs Σ_1 and Σ_2 is illustrated in Fig. 1.

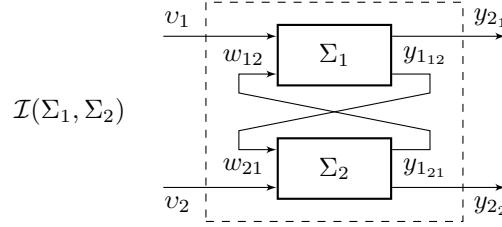


FIGURE 1. Interconnection of two POMDPs Σ_1 and Σ_2 .

5. COMPOSITIONAL CONSTRUCTION OF CBF

In this section, we analyze networks of POMDP and provide a compositional approach to construct a CBF of an interconnected POMDP based on LCBF of its subsystems. For $i \in \{1, \dots, N\}$, consider the PO-dt-SCS Σ_i in (2.2), its corresponding estimator $\hat{\Sigma}_i$ in (2.5), and the augmented system $\tilde{\Sigma}$ in (3.1). Assume there exists a LCBF \mathcal{B}_i as defined in Definition 3.1 or 3.9 with functions $\alpha_i \in \mathcal{K}_\infty$, $\rho_i \in \mathcal{K}_\infty \cup \{0\}$ and constants $\bar{\lambda}_i, \bar{\psi}_i \in \mathbb{R}_{\geq 0}$, $\bar{\gamma}_i \in \mathbb{R}_{> 0}$, and $0 < \bar{\kappa}_i < 1$. Now we raise the following small-gain assumption that is essential for the compositionality results of this section.

Assumption 2. Assume that \mathcal{K}_∞ functions $\bar{\kappa}_{ij}$ defined as

$$\bar{\kappa}_{ij}(s) := \begin{cases} \bar{\kappa}_i(s), & \text{if } i = j, \\ \rho_i(\alpha_j^{-1}(s)), & \text{if } i \neq j, \end{cases}$$

satisfy

$$\bar{\kappa}_{i_1 i_2} \circ \bar{\kappa}_{i_2 i_3} \circ \dots \circ \bar{\kappa}_{i_{r-1} i_r} \circ \bar{\kappa}_{i_r i_1} < \mathcal{I}_d, \quad (5.1)$$

for all sequences $(i_1, \dots, i_r) \in \{1, \dots, N\}^r$ and $r \in \{1, \dots, N\}$.

Remark 5.1. Note that the small-gain condition (5.1) is a standard one in studying the stability of large-scale interconnected systems via ISS Lyapunov functions [DRW07, DRW10]. This condition is automatically satisfied if each $\bar{\kappa}_{ij}$ is less than identity ($\bar{\kappa}_{ij} < \mathcal{I}_d, \forall i, j \in \{1, \dots, N\}$).

The small-gain condition (5.1) implies the existence of \mathcal{K}_∞ functions $\sigma_i > 0$ [Rüf10, Theorem 5.5], satisfying

$$\max_{i,j} \{\sigma_i^{-1} \circ \bar{\kappa}_{ij} \circ \sigma_j\} < \mathcal{I}_d, \quad i, j = \{1, \dots, N\}. \quad (5.2)$$

In the next theorem, we show that if Assumption 2 holds and $\max_i \sigma_i^{-1}$ is concave (in order to employ Jensen's inequality), then one can compute a CBF for the interconnected system Σ as in Definition 3.2 in a compositional fashion.

Theorem 5.2. Consider the interconnected POMDP $\Sigma = \mathcal{I}(\Sigma_1, \dots, \Sigma_N)$ induced by $N \in \mathbb{N}_{\geq 1}$ subsystems Σ_i . Suppose that for each Σ_i there exists an estimator $\widehat{\Sigma}_i$ together with a corresponding LCBF \mathcal{B}_i as defined in Definition 3.1 with initial and unsafe sets X_{a_i} and X_{b_i} , respectively. If Assumption 2 holds and $\max_i \sigma_i^{-1}$ for σ_i as in (5.2) is concave and

$$\max_i \{\sigma_i^{-1}(\bar{\gamma}_i)\} < \max_i \{\sigma_i^{-1}(\bar{\lambda}_i)\}, \quad (5.3)$$

then function $\mathcal{B}(x, \hat{x})$ defined as

$$\mathcal{B}(x, \hat{x}) := \max_i \{\sigma_i^{-1}(\mathcal{B}_i(x_i, \hat{x}_i))\}, \quad (5.4)$$

is a CBF for the augmented system $\widetilde{\Sigma} = [\Sigma ; \widehat{\Sigma}]$ with initial and unsafe sets $X_a = \prod_{i=1}^N X_{a_i}$, $X_b = \prod_{i=1}^N X_{b_i}$, respectively.

The proof of Theorem 5.2 is provided in Appendix.

Similarly, we propose the next theorem to compute a CBF for an interconnected system Σ as in Definition 3.10 in a compositional way based on LCBFs of subsystems.

Theorem 5.3. Consider an interconnected POMDP $\Sigma = \mathcal{I}(\Sigma_1, \dots, \Sigma_N)$ induced by $N \in \mathbb{N}_{\geq 1}$ subsystems Σ_i . Suppose that for each Σ_i there exists an estimator $\widehat{\Sigma}_i$ together with a corresponding LCBF \mathcal{B}_i as defined in Definition 3.9 with initial and unsafe sets X_{a_i} and $X_{b_i}^\epsilon$, respectively. If Assumption 2 holds and $\max_i \sigma_i^{-1}$ for σ_i as in (5.2) is concave and

$$\max_i \{\sigma_i^{-1}(\bar{\gamma}_i)\} < \max_i \{\sigma_i^{-1}(\bar{\lambda}_i)\}, \quad (5.5)$$

then function $\mathcal{B}(x)$ defined as

$$\mathcal{B}(x) := \max_i \{\sigma_i^{-1}(\mathcal{B}_i(x_i))\}, \quad (5.6)$$

is a CBF for the estimator $\widehat{\Sigma} = \mathcal{I}(\widehat{\Sigma}_1, \dots, \widehat{\Sigma}_N)$ with initial and unsafe sets $X_a = \prod_{i=1}^N X_{a_i}$, $X_b^\epsilon = \prod_{i=1}^N X_{b_i}^\epsilon$, respectively.

The proof of Theorem 5.3 follows the same reasoning as that of Theorem 5.2 and is omitted here due to lack of space.

Finally, we provide an approach to compositionally construct an SSF for an interconnected POMDP Σ based on SPSFs of its subsystems. Note that the constructed SSF is one of the main ingredients used in Theorem 3.11. First, we raise the following small-gain assumption.

Assumption 3. Assume that \mathcal{K}_∞ functions μ_{ij} defined as

$$\bar{\mu}_{ij}(s) := \begin{cases} \bar{\mu}_i(s), & \text{if } i = j, \\ \varrho_i(\varepsilon_j^{-1}(s)), & \text{if } i \neq j, \end{cases}$$

satisfy

$$\bar{\mu}_{i_1 i_2} \circ \bar{\mu}_{i_2 i_3} \circ \dots \circ \bar{\mu}_{i_{r-1} i_r} \circ \bar{\mu}_{i_r i_1} < \mathcal{I}_d, \quad (5.7)$$

for all sequences $(i_1, \dots, i_r) \in \{1, \dots, N\}^r$ and $r \in \{1, \dots, N\}$.

The small-gain condition (5.7) implies the existence of \mathcal{K}_∞ functions $\zeta_i > 0$ [Rüf10, Theorem 5.5], satisfying

$$\max_{i,j} \{\zeta_i^{-1} \circ \bar{\mu}_{ij} \circ \zeta_j\} < \mathcal{I}_d, \quad i, j = \{1, \dots, N\}. \quad (5.8)$$

In the next proposition, we show that if Assumption 3 holds and $\max_i \zeta_i^{-1}$ is concave, then we can compositionally construct an SSF for an interconnected system based on SPSFs of its subsystems.

Proposition 5.4. Consider an interconnected POMDP $\Sigma = \mathcal{I}(\Sigma_1, \dots, \Sigma_N)$ induced by $N \in \mathbb{N}_{\geq 1}$ subsystems Σ_i . Suppose that for each Σ_i there exists an estimator $\widehat{\Sigma}_i$ together with a corresponding SPSF $\phi_i(x_i, \hat{x}_i)$. If Assumption 3 holds and $\max_i \zeta_i^{-1}$ for ζ_i as in (5.8) is concave, then the function $\phi(x, \hat{x})$ defined as

$$\phi(x, \hat{x}) := \max_i \{\zeta_i^{-1}(\phi_i(x_i, \hat{x}_i))\},$$

is an SSF from $\widehat{\Sigma} = \mathcal{I}(\widehat{\Sigma}_1, \dots, \widehat{\Sigma}_N)$ to $\Sigma = \mathcal{I}(\Sigma_1, \dots, \Sigma_N)$, as defined in Definition 3.7, with

$$\begin{aligned}\mu(s) &= \max_{i,j} \{ \zeta_i^{-1} \circ \bar{\mu}_{ij} \circ \zeta_j(s) \}, \quad i, j = \{1, \dots, N\}, \\ c &= \max_i \zeta_i^{-1}(\bar{c}_i).\end{aligned}$$

The proof of Proposition 5.4 follows the same reasoning as that of Theorem 5.2 and is omitted here.

6. COMPUTATION OF LCBF

In this subsection, we provide a systematic approach to search for LCBFs and the corresponding control policies for subsystems. The proposed approach is based on the sum-of-squares (SOS) optimization problem [Par03], in which LCBF is restricted to be non-negative which can be written as a sum of squares of different polynomials. To do so, we need to raise the following assumption.

Assumption 4. *The POMDP $\Sigma = (X, U, W, \varsigma_1, f, Y_1, Y_2, h_1, h_2, \varsigma_2)$ has a continuous state set $X \subseteq \mathbb{R}^n$ and continuous external and internal input sets $U \subseteq \mathbb{R}^m$ and $W \in \mathbb{R}^p$. Moreover, the transition map $f : X \times U \times W \times V_{\varsigma_1} \rightarrow X$ is a polynomial function of its arguments. We also assume that the internal output map $h_1 : X \rightarrow Y_1$ and \mathcal{K}_∞ functions α and ρ are polynomial.*

Under Assumption 4, one can reformulate conditions of Definition 3.1 and Definition 3.9 to an SOS optimization problem in order to search for a polynomial LCBF $\mathcal{B}_i(\cdot, \cdot)$ and $\mathcal{B}_i(\cdot)$, and their corresponding control policies. In the following Lemmas, SOS formulations are provided.

Lemma 6.1. *Suppose Assumption 4 holds and sets X_a, X_b, X, W can be defined by vectors of polynomial inequalities $X_a = \{x \in \mathbb{R}^n \mid g_a(x) \geq 0\}$, $X_b = \{x \in \mathbb{R}^n \mid g_b(x) \geq 0\}$, $X = \{x \in \mathbb{R}^n \mid g(x) \geq 0\}$, and $W = \{w \in \mathbb{R}^p \mid g_w(w) \geq 0\}$, where the inequalities are defined element-wise. Suppose there exists a sum-of-square polynomial $\mathcal{B}(x, \hat{x})$, constants $\bar{\gamma}, \bar{\psi} \in \mathbb{R}_{\geq 0}$, $\bar{\lambda} \in \mathbb{R}_{>0}$, $0 < \bar{\kappa} < 1$, functions $\alpha \in \mathcal{K}_\infty$, $\bar{\rho} \in \mathcal{K}_\infty \cup \{0\}$, polynomials $l_{v_j}(\hat{x}, \hat{w})$ corresponding to the j^{th} input in $v(k) = (v_1(k), v_2(k), \dots, v_m(k)) \in U \subseteq \mathbb{R}^m$, and vectors of sum-of-squares polynomials $l_z(x), \hat{l}_z(\hat{x})$ for $z \in \{0, 1, 2, 3\}$, and $l_w(w), \hat{l}_w(\hat{w})$, of appropriate dimensions such that the following expressions are sum-of-square polynomials:*

$$\mathcal{B}(x, \hat{x}) - [l_0^T(x) \quad \hat{l}_0^T(\hat{x})] \begin{bmatrix} g(x) \\ g(\hat{x}) \end{bmatrix} - \alpha \left(\begin{bmatrix} h_1(x) \\ h_1(\hat{x}) \end{bmatrix}^T \begin{bmatrix} h_1(x) \\ h_1(\hat{x}) \end{bmatrix} \right), \quad (6.1)$$

$$- \mathcal{B}(x, \hat{x}) - [l_1^T(x) \quad \hat{l}_1^T(\hat{x})] \begin{bmatrix} g_a(x) \\ g_a(\hat{x}) \end{bmatrix} + \bar{\lambda}, \quad (6.2)$$

$$\mathcal{B}(x, \hat{x}) - [l_2^T(x) \quad \hat{l}_2^T(\hat{x})] \begin{bmatrix} g_b(x) \\ g(\hat{x}) \end{bmatrix} + \bar{\gamma}, \quad (6.3)$$

$$\begin{aligned} & - \mathbb{E} \left[\mathcal{B}(f(x(k), v(k), w(k), \varsigma_1(k)), \hat{f}(\hat{x}(k), v(k), \hat{w}(k), y_2(k))), \mid x(k), \hat{x}(k), v(k), w(k), \hat{w}(k)) \right] + \bar{\kappa} \mathcal{B}(x(k), \hat{x}(k)) \\ & + \bar{\rho} \left(\frac{\begin{bmatrix} w(k) \\ \hat{w}(k) \end{bmatrix}^T \begin{bmatrix} w(k) \\ \hat{w}(k) \end{bmatrix}}{2p} \right) + \bar{\psi} \sum_{j=1}^m (v_j(k) - l_{v_j}(\hat{x}(k), \hat{w}(k))) - [l_3^T(x(k)) \quad \hat{l}_3^T(\hat{x}(k))] \begin{bmatrix} g(x(k)) \\ g(\hat{x}(k)) \end{bmatrix} \\ & - [l_w^T(w(k)) \quad \hat{l}_w^T(\hat{w}(k))] \begin{bmatrix} g_w(w(k)) \\ g_w(\hat{w}(k)) \end{bmatrix}, \end{aligned} \quad (6.4)$$

where p is the dimension of the internal inputs w and \hat{w} . Then $\mathcal{B}(x, \hat{x})$ satisfies conditions (3.2)-(3.15) in Definition 3.1 and $v(k) = [l_{v_1}(\hat{x}(k), \hat{w}(k)); \dots; l_{v_m}(\hat{x}(k), \hat{w}(k))]$ is the corresponding safety controller, with

$$\begin{aligned}\bar{\kappa} &= \mathcal{I}_d - (\mathcal{I}_d - \pi_1) \circ (\mathcal{I}_d - \bar{\kappa}), \\ \rho &= (\mathcal{I}_d + \pi_2) \circ (\mathcal{I}_d - \bar{\kappa})^{-1} \circ \pi_1^{-1} \circ \pi_3 \circ \bar{\rho}, \\ \bar{\psi} &= (\mathcal{I}_d + \pi_2^{-1}) \circ (\mathcal{I}_d - \bar{\kappa})^{-1} \circ \pi_1^{-1} \circ \pi_3 \circ (\pi_3 - \mathcal{I}_d)^{-1} \circ (\bar{\psi}),\end{aligned}$$

where π_1, π_2, π_3 being some arbitrarily chosen \mathcal{K}_∞ functions so that $(\mathcal{I}_d - \pi_1) \in \mathcal{K}_\infty$, and $(\pi_3 - \mathcal{I}_d) \in \mathcal{K}_\infty$.

The proof follows the same argument as in [JSZ20, Lemma 5.9], and is omitted here due to lack of space.

Remark 6.2. Inequalities (3.2) and (3.5) consider infinity norms over $[h_1(x); h_1(\hat{x})]$ and $[w; \hat{w}]$, respectively. Since such norms cannot be expressed as polynomials, we convert infinity norms to Euclidean ones and that is the reason constant $2p$ appears as a denominator in (6.4).

We now state another lemma for the computation of LCBF as in Definition 3.9.

Lemma 6.3. Suppose Assumption 4 holds and sets $X_a, X_b^\epsilon, X, W, Y_2$ can be defined by vectors of polynomial inequalities $X_a = \{x \in \mathbb{R}^n \mid g_a(x) \geq 0\}$, $X_b^\epsilon = \{x \in \mathbb{R}^n \mid g_b^\epsilon(x) \geq 0\}$, $X = \{x \in \mathbb{R}^n \mid g(x) \geq 0\}$, $W = \{w \in \mathbb{R}^p \mid g_w(w) \geq 0\}$, and $Y_2 = \{y_2 \in \mathbb{R}^q \mid g_y(y_2) \geq 0\}$ where the inequalities are defined element-wise. Suppose there exists a sum-of-square polynomial $\mathcal{B}(x)$, constants $\bar{\gamma}, \bar{\psi} \in \mathbb{R}_{\geq 0}, \bar{\lambda} \in \mathbb{R}_{> 0}, 0 < \bar{\kappa} < 1$, functions $\alpha \in \mathcal{K}_\infty, \bar{\rho} \in \mathcal{K}_\infty \cup \{0\}$, polynomials $l_{v_j}(\hat{x}, \hat{w})$ corresponding to the j^{th} input in $v(k) = (v_1(k), v_2(k), \dots, v_m(k)) \in U \subseteq \mathbb{R}^m$, and vectors of sum-of-squares polynomials $l_z(x)$ for $z \in \{0, 1, 2\}$, $\hat{l}_3(\hat{x}), \hat{l}_w(\hat{w})$ and $l_y(y_2)$ of appropriate dimensions such that the following expressions are sum-of-square polynomials:

$$\mathcal{B}(x) - l_0^T(x)g(x) - \alpha(h_1(x)^T h_1(x)), \quad (6.5)$$

$$-\mathcal{B}(x) - l_1^T(x)g_a(x) + \bar{\lambda}, \quad (6.6)$$

$$\mathcal{B}(x) - l_2^T(x)g_b^\epsilon(x) + \bar{\gamma}, \quad (6.7)$$

$$\begin{aligned}& -\mathbb{E}\left[\mathcal{B}(\hat{f}(\hat{x}(k), v(k), \hat{w}(k), y_2(k))) \mid \hat{x}(k), v(k), \hat{w}(k)\right] + \bar{\kappa}\mathcal{B}(\hat{x}(k)) + \bar{\rho}\left(\frac{\hat{w}^T(k)\hat{w}(k)}{p}\right) + \bar{\psi} \\ & - \sum_{j=1}^m (v_j(k) - l_{v_j}(\hat{x}(k), \hat{w}(k))) - \hat{l}_3^T(\hat{x}(k))g(\hat{x}(k)) - \hat{l}_w^T(\hat{w}(k))g_w(\hat{w}(k)) - l_y^T(y_2(k))g_y(y_2(k)),\end{aligned} \quad (6.8)$$

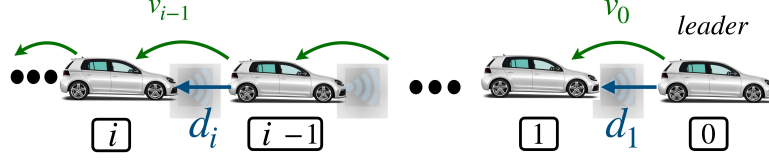
where p is the dimension of the internal input w . Then $\mathcal{B}(\hat{x})$ satisfies conditions (3.12)-(3.15) in Definition 3.9 and $v(k) = [l_{v_1}(\hat{x}(k), \hat{w}(k)); \dots; l_{v_m}(\hat{x}(k), \hat{w}(k))]$ is the corresponding safety controller, where $\bar{\kappa}, \bar{\rho}, \bar{\psi}$ can be acquired based on $\bar{\kappa}, \bar{\rho}, \bar{\psi}$ similar to Lemma 6.1.

Remark 6.4. In order to compute the sum-of-square polynomials $\mathcal{B}(x, \hat{x})$ and $\mathcal{B}(x)$ fulfilling reformulated conditions (6.1)-(6.4), and (6.5)-(6.8), one can employ existing software tools such as SOSTOOLS [PPP02] together with a semidefinite programming solver such as SeDuMi [Stu99].

7. CASE STUDY

In this section, we illustrate our proposed results by applying them to an adaptive cruise control (ACC) system consisting of N vehicles in a platoon (see Fig. 2). This model is adapted from [SSGB17]. The evolution of states can be described by the interconnected PO-dt-SCS

$$\Sigma: \begin{cases} x(k+1) = \bar{A}x(k) + \bar{B}v(k) + \varsigma_1(k), \\ y(k) = \bar{C}x(k) + \varsigma_2(k), \end{cases}$$

FIGURE 2. Platoon model for $N = 1000$ vehicles.

where \bar{A} is a block matrix with diagonal blocks A , and off-diagonal blocks $A_{i(i-1)} = A_w, i \in \{2, \dots, N\}$, where

$$A = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}, \quad A_w = \begin{bmatrix} 0 & \tau \\ 0 & 0 \end{bmatrix},$$

with $\tau = 0.01$ being the interconnection degree, and all other off-diagonal blocks being zero matrices of appropriate dimensions. Moreover, \bar{B} is a partitioned matrix with main diagonal blocks $B = [0 \ 1]$, and all other off-diagonal blocks being zero matrices of appropriate dimensions. The matrix \bar{C} is a partitioned matrix with main diagonal blocks $C = [1 \ 0]^T$ and all other off-diagonal blocks being zero matrices of appropriate dimensions. Moreover, $x(k) = [x_1(k); \dots; x_N(k)]$, $v(k) = [v_1(k); \dots; v_N(k)]$, $\varsigma_1(k) = [\varsigma_{1_1}(k); \dots; \varsigma_{1_N}(k)]$, and $\varsigma_2(k) = [\varsigma_{2_1}(k); \dots; \varsigma_{2_N}(k)]$. Let us consider each individual vehicle Σ_i described as

$$\Sigma_i : \begin{cases} x_i(k+1) = Ax_i(k) + Bv_i(k) + A_w w_i(k) + \varsigma_{1_i}(k), \\ y_{1_i}(k) = C_1 x_i(k), \\ y_{2_i}(k) = C_2 x_i(k) + \varsigma_{2_i}, \end{cases}$$

where $y_{1_i}(k) = y_{1_{i(i+1)}}(k) = C_1 x_i(k), i \in \{1, \dots, N\}$, (with $C_1 = [0 \ 1]$ and $y_{1_{N(N+1)}} = 0$) and $C_2 = C$. One can readily verify that $\Sigma = \mathcal{I}(\Sigma_1, \dots, \Sigma_N)$, where $w_i(k) = [0; w_{i(i-1)}(k)], i \in \{1, \dots, N\}$, (with $w_{i(i-1)} = y_{1_{(i-1)i}} = C_1 x_{i-1}, w_{1,0} = 0$). The state of the i -th vehicle is defined as $x_i = [d_i; v_i]$, for $i \in \{1, \dots, N\}$, where d_i denotes the relative distance between the vehicle i and its preceding vehicle $i-1$ (the 0-th vehicle represents the leader), v_i is its velocity in the leader's frame, and $v_i \in [-1, 1]$ is the bounded control input. The overall control objective in ACC is for each vehicle to adjust its speed in order to maintain a safe distance from the vehicle ahead [JF18]. For the system Σ_i , we design a proper estimator of the following form

$$\hat{\Sigma}_i : \begin{cases} \hat{x}_i(k+1) = A\hat{x}_i(k) + Bv_i(k) + A_w \hat{w}_i(k) + K(y_{2_i}(k) - C_2 \hat{x}_i(k)), \\ \hat{y}_{1_i}(k) = C_1 \hat{x}_i(k), \end{cases}$$

where $K = [1.7; -0.72]$ is the estimator gain. We consider a network of $N = 1000$ vehicles where the regions of interest for each vehicle are $X \in [0, 3.5] \times [-2, 3]$, $X_a \in [1, 1.5] \times [-0.4, 0.4]$, and $X_b \in [0, 0.5] \times [-2, -1.5] \cup [3, 3.5] \times [2.5, 3]$. Now, for each vehicle we compute LCBFs while compositionally synthesizing safety controllers for a bounded-time horizon. We construct LCBFs using the two methods introduced in Section 3 and employ the software SOSTOOLS to search for LCBFs as described in Section 6. According to Section 3.1, we compute the LCBF $\mathcal{B}_i(x_i, \hat{x}_i)$ of an order 4 and its corresponding controller as the following:

$$v_i = 0.06\hat{d}_i - 0.7\hat{v}_i + 0.02\hat{v}_{i-1} - 0.07, \quad (7.1)$$

for $i \in \{1, \dots, N\}$. Moreover, the corresponding constants and functions in Definition 3.1 are quantified as $\alpha_i(s) = 10^{-5}s, s \in \mathbb{R}_{\geq 0}, \bar{\gamma}_i = 0.12, \bar{\lambda}_i = 1, \bar{\kappa}_i = 0.95, \rho_i(s) = 2 \times 10^{-8}s, s \in \mathbb{R}_{\geq 0}, \bar{\psi}_i = 0.001$. Now, we check the small gain condition (5.1) that is required for the compositionality result. By taking $\sigma_i(s) = s, i \in \{1, \dots, N\}$, the condition (5.1), and as a result the condition (5.2) are always satisfied without any restriction on the number of vehicles. Hence, $\mathcal{B}(x, \hat{x}) = \max_i \mathcal{B}_i(x_i, \hat{x}_i)$ is a CBF for Σ satisfying conditions in Definition 3.2 with $\gamma = 0.12, \lambda = 1, \kappa = 0.95, \psi = 0.001$. By employing Theorem 3.4, one can guarantee that states of the interconnected system starting from X_a remain in the safe set $X \setminus X_b$ within the time horizon $T_d = 10$ with

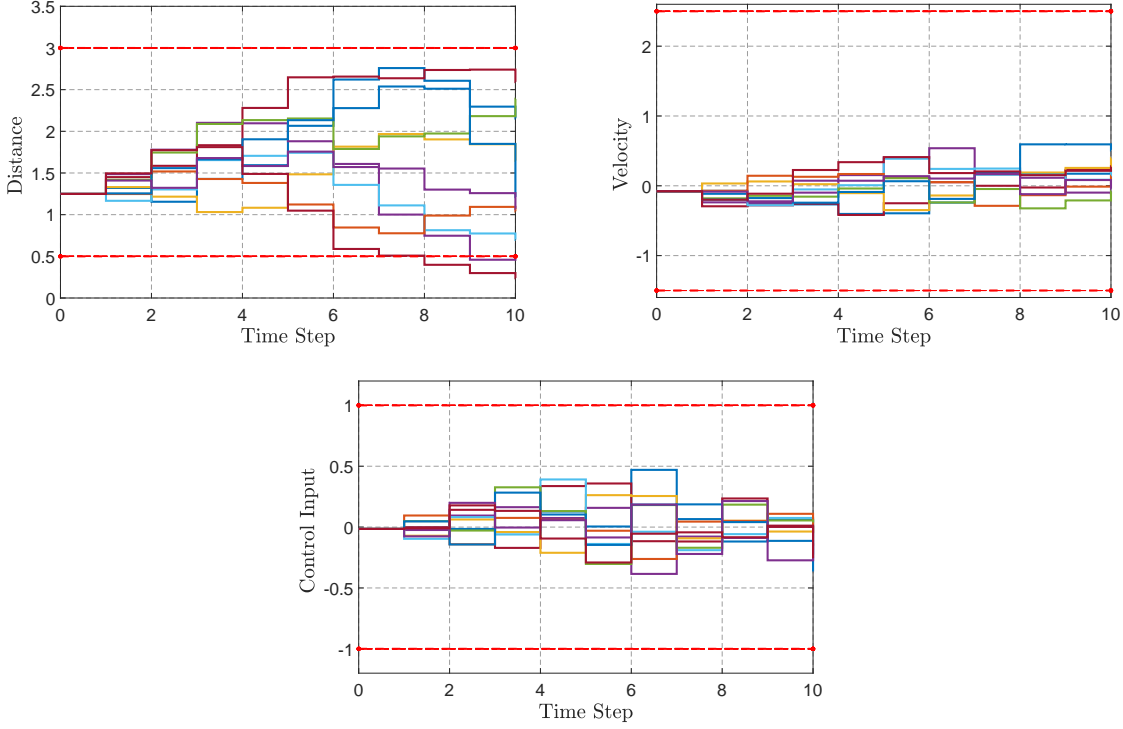


FIGURE 3. Closed-loop state (distance and velocity) and input trajectories of a representative vehicle with different noise realizations in a network of 1000 vehicles under controller (7.1).

a probability of at least 87.12%. Closed-loop state and input trajectories of a representative vehicle with different noise realizations are illustrated in Fig. 3 with only 10 trajectories.

We now construct the LCBF $\mathcal{B}_i(\hat{x}_i)$ of an order 4 for the estimator, as described in Section 3.2, and compute its corresponding controller as

$$v_i = 0.09\hat{d}_i - \hat{v}_i + 0.03\hat{v}_{i-1} - 0.09, \quad (7.2)$$

for $i \in \{1, \dots, N\}$. The corresponding constants and functions in Definition 3.9 are quantified as $\alpha_i(s) = 10^{-5}s$, $s \in \mathbb{R}_{\geq 0}$, $\bar{\gamma}_i = 0.12$, $\bar{\lambda}_i = 1$, $\bar{\kappa}_i = 0.95$, $\rho_i(s) = 2 \times 10^{-8}s$, $s \in \mathbb{R}_{\geq 0}$, $\bar{\psi}_i = 0.001$. Similar to the first method, we check the small gain condition (5.1) for the compositionality result. By taking $\sigma_i(s) = s$, $i \in \{1, \dots, N\}$, the condition (5.1), and as a result the condition (5.2) are both satisfied. Hence, $\mathcal{B}(\hat{x}) = \max_i \mathcal{B}_i(\hat{x}_i)$ is a CBF for Σ satisfying conditions in Definition 3.10 with $\gamma = 0.12$, $\lambda = 1$, $\kappa = 0.95$, $\psi = 0.001$. By employing the result of Theorem 3.4, one can guarantee that the states of the estimator starting from X_a will not reach X_b^ϵ within the time horizon $T_d = 10$ with a probability of at least 87.12%. Now, in order to compute the exit probability bound for the interconnected system, we search for an SPSF of a quadratic form $\phi_i(x_i, \hat{x}_i) = (x_i - \hat{x}_i)^T M (x_i - \hat{x}_i)$, where M is a positive-definite matrix. Since the dynamic of the system is linear, the conditions in Definition 3.6 reduce to solving the following matrix inequality:

$$(1 + 2/\tilde{\pi})(A - KC_2)^T M (A - KC_2) \leq \bar{\mu}M,$$

where K is the estimator gain, and $\tilde{\pi} > 0$. By using the tool YALMIP [Lof04], we compute M as

$$M = \begin{bmatrix} 0.0257 & 0.0259 \\ 0.0259 & 0.0262 \end{bmatrix},$$

with $\tilde{\pi} = 1$. The functions and constants associated with this SPSF are computed by following the compositional construction method for linear systems introduced in [LSZ20d, Theorem 6.10] as $\varepsilon(s) = 0.3s^2$, $s \in$

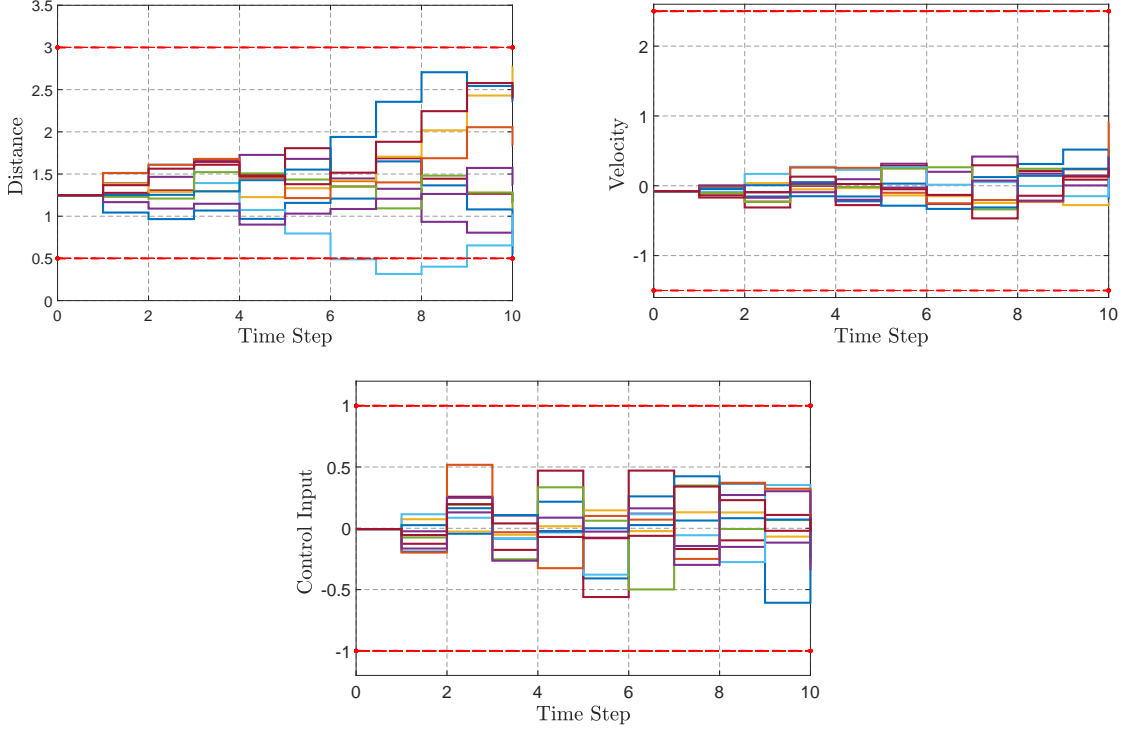


FIGURE 4. Closed-loop state (distance and velocity) and input trajectories of a representative vehicle with different noise realizations in a network of 1000 vehicles under controller (7.2).

$\mathbb{R}_{\geq 0}$, $\bar{\mu} = 0.4$, $\varrho(s) = 0.002s^2$, $s \in \mathbb{R}_{\geq 0}$, $\bar{c} = 10^{-5}$. Hence, $\phi(x, \hat{x}) = \max_i \phi_i(x_i, \hat{x}_i)$ is an SSF from $\hat{\Sigma}$ to Σ satisfying the conditions in Definition 3.7 with $\varepsilon(s) = 0.3s^2$, $s \in \mathbb{R}_{\geq 0}$, $\mu = 0.4$, $c = 10^{-5}$, $\epsilon = 0.01$. An upper bound of 3.61% on the probability of the estimation accuracy is computed according to Theorem 3.8 within the time horizon $T_d = 10$. Employing Theorem 3.11, the probability that the solution process of the system starting from the initial region X_a and not reaching X_b is at least 83.51%. Closed-loop state and input trajectories of a representative vehicle with different noise realizations are illustrated in Fig. 4.

8. CONCLUSIONS

In this paper, we proposed a compositional approach based on control barrier functions for the synthesis of safety controllers for networks of POMDP by utilizing small-gain type reasoning. The proposed scheme provides an upper bound on the probability that the interconnected system reaches an unsafe region in a finite-time horizon. In this respect, we first quantified probability bounds without any prior information of the estimation accuracy. This is achieved by constructing local barrier functions over an augmented system composed of subsystems and their corresponding estimators. Alternatively, we formulated local barrier functions based on only estimators' dynamics and computed the exit probability by utilizing the probability bound on the estimation accuracy computed via notions of stochastic simulation functions. We finally demonstrated the effectiveness of our proposed results by applying them to an adaptive cruise control problem.

REFERENCES

- [ACE⁺19] Aaron D Ames, Samuel Coogan, Magnus Egerstedt, Gennaro Notomista, Koushil Sreenath, and Paulo Tabuada. Control barrier functions: Theory and applications. In *2019 18th European Control Conference (ECC)*, pages 3420–3431. IEEE, 2019.

- [ALZ20] M. Anand, A. Lavaei, and M. Zamani. Compositional construction of control barrier certificates for large-scale interconnected stochastic systems. In *21st IFAC World Conference*, 2020.
- [ALZ21] M. Anand, A. Lavaei, and M. Zamani. From small-gain theory to compositional construction of barrier certificates for large-scale stochastic systems. *arXiv:2101.06916*, 2021.
- [AXGT16] Aaron D Ames, Xiangru Xu, Jessy W Grizzle, and Paulo Tabuada. Control barrier function based quadratic programs for safety critical systems. *IEEE Transactions on Automatic Control*, 62(8):3861–3876, 2016.
- [Cla19] Andrew Clark. Control barrier functions for complete and incomplete information stochastic systems. In *2019 American Control Conference (ACC)*, pages 2928–2935. IEEE, 2019.
- [DRW07] S. Dashkovskiy, B. S. Rüffer, and F. R. Wirth. An ISS small gain theorem for general networks. *Mathematics of Control, Signals, and Systems (MCSS)*, 19(2):93–122, 2007.
- [DRW10] Sergey N Dashkovskiy, Björn S Rüffer, and Fabian R Wirth. Small gain theorems for large scale systems and construction of ISS Lyapunov functions. *SIAM Journal on Control and Optimization*, 48(6):4089–4118, 2010.
- [JF18] Niloofar Jahanshahi and Riccardo MG Ferrari. Attack detection and estimation in cooperative vehicles platoons: A sliding mode observer approach. *IFAC-PapersOnLine*, 51(23):212–217, 2018.
- [JJZ20a] Niloofar Jahanshahi, Pushpak Jagtap, and Majid Zamani. Synthesis of partially observed jump-diffusion systems via control barrier functions. *IEEE Control Systems Letters*, 5(1):253–258, 2020.
- [JJZ20b] Niloofar Jahanshahi, Pushpak Jagtap, and Majid Zamani. Synthesis of stochastic systems with partial information via control barrier functions. *21st IFAC World Congress*, 2020.
- [JSZ20] Pushpak Jagtap, Abdalla Swikir, and Majid Zamani. Compositional construction of control barrier functions for interconnected control systems. In *Proceedings of the 23rd International Conference on Hybrid Systems: Computation and Control*, pages 1–11, 2020.
- [Kal97] O. Kallenberg. *Foundations of modern probability*. Springer-Verlag, New York, 1997.
- [Kus65] Harold J Kushner. On the stability of stochastic dynamical systems. *Proceedings of the National Academy of Sciences of the United States of America*, 53(1):8, 1965.
- [Kus67] Harold J Kushner. Stochastic stability and control. Technical report, Brown Univ Providence RI, 1967.
- [L⁺96] John Lygeros et al. *Hierarchical, hybrid control of large scale systems*. PhD thesis, Citeseer, 1996.
- [Lav19] A. Lavaei. *Automated Verification and Control of Large-Scale Stochastic Cyber-Physical Systems: Compositional Techniques*. PhD thesis, Department of Electrical Engineering, Technische Universität München, Germany, 2019.
- [Lof04] Johan Lofberg. Yalmip: A toolbox for modeling and optimization in matlab. In *2004 IEEE international conference on robotics and automation (IEEE Cat. No. 04CH37508)*, pages 284–289. IEEE, 2004.
- [LSAZ20] A. Lavaei, S. Soudjani, A. Abate, and M. Zamani. Automated verification and synthesis of stochastic hybrid systems: A survey. *Automatica, accepted as a survey paper proposal, arXiv:2101.07491*, 2020.
- [LSZ18] A. Lavaei, S. Soudjani, and M. Zamani. From dissipativity theory to compositional construction of finite Markov decision processes. In *Proceedings of the 21st ACM International Conference on Hybrid Systems: Computation and Control*, pages 21–30, 2018.
- [LSZ19] A. Lavaei, S. Soudjani, and M. Zamani. Compositional construction of infinite abstractions for networks of stochastic control systems. *Automatica*, 107:125–137, 2019.
- [LSZ20a] A. Lavaei, S. Soudjani, and M. Zamani. Compositional abstraction-based synthesis for networks of stochastic switched systems. *Automatica*, 114, 2020.
- [LSZ20b] A. Lavaei, S. Soudjani, and M. Zamani. Compositional abstraction-based synthesis of general MDPs via approximate probabilistic relations. *Nonlinear Analysis: Hybrid Systems*, 39, 2020.
- [LSZ20c] A. Lavaei, S. Soudjani, and M. Zamani. Compositional abstraction of large-scale stochastic systems: A relaxed dissipativity approach. *Nonlinear Analysis: Hybrid Systems*, 36, 2020.
- [LSZ20d] A. Lavaei, S. Soudjani, and M. Zamani. Compositional (in)finite abstractions for large-scale interconnected stochastic systems. *IEEE Transactions on Automatic Control*, 65(12):5280–5295, 2020.
- [LWL09] Jinling Liang, Zidong Wang, and Xiaohui Liu. State estimation for coupled uncertain stochastic networks with missing measurements and time-varying delays: the discrete-time case. *IEEE Transactions on Neural Networks*, 20(5):781–793, 2009.
- [LZ19] A. Lavaei and M. Zamani. Compositional construction of finite MDPs for large-scale stochastic switched systems: A dissipativity approach. *Proceedings of the 15th IFAC Symposium on Large Scale Complex Systems: Theory and Applications*, 52(3):31–36, 2019.
- [NSZ20a] A. Nejati, S. Soudjani, and M. Zamani. Compositional construction of control barrier certificates for large-scale stochastic switched systems. *IEEE Control Systems Letters*, 4(4):845–850, 2020.
- [NSZ20b] A. Nejati, S. Soudjani, and M. Zamani. Compositional construction of control barrier functions for continuous-time stochastic hybrid systems. *arXiv:2012.07296*, 2020.
- [NSZ20c] A. Nejati, S. Soudjani, and M. Zamani. Compositional construction of control barrier functions for networks of continuous-time stochastic systems. In *Proceedings of the 21st IFAC World Congress*, 2020.
- [NSZ21] A. Nejati, S. Soudjani, and M. Zamani. Compositional abstraction-based synthesis for continuous-time stochastic hybrid systems. *European Journal of Control*, 57:82–94, 2021.
- [NZ20] A. Nejati and M. Zamani. Compositional construction of finite MDPs for continuous-time stochastic systems: A dissipativity approach. In *Proceedings of the 21st IFAC World Congress*, 2020.

- [Par03] Pablo A Parrilo. Semidefinite programming relaxations for semialgebraic problems. *Mathematical programming*, 96(2):293–320, 2003.
- [PJP07] 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*, 52(8):1415–1428, 2007.
- [PPP02] Stephen Prajna, Antonis Papachristodoulou, and Pablo A Parrilo. Introducing SOSTOOLS: A general purpose sum of squares programming solver. *Proceedings of the 41st IEEE Conference on Decision and Control, 2002.*, pages 741–746, 2002.
- [RGYU00] Konrad Reif, Stefan Gunther, Engin Yaz, and Rolf Unbehauen. Stochastic stability of the continuous-time extended kalman filter. *IEE Proceedings-Control Theory and Applications*, 147(1):45–52, 2000.
- [Rüf10] Björn S Rüffer. Monotone inequalities, dynamical systems, and paths in the positive orthant of euclidean n-space. *Positivity*, 14(2):257–283, 2010.
- [SAM17] S. Soudjani, A. Abate, and R. Majumdar. Dynamic Bayesian networks for formal verification of structured stochastic processes. *Acta Informatica*, 54(2):217–242, 2017.
- [SSGB17] S. Sadraddini, S. Sivaranjani, V. Gupta, and C. Belta. Provably safe cruise control of vehicular platoons. *IEEE Control Systems Letters*, 1(2):262–267, 2017.
- [SSS09] Srdjan S Stanković, Miloš S Stanković, and Dušan M Stipanović. Consensus based overlapping decentralized estimation with missing observations and communication faults. *Automatica*, 45(6):1397–1406, 2009.
- [Stu99] Jos F Sturm. Using sedumi 1.02, a matlab toolbox for optimization over symmetric cones. *Optimization methods and software*, pages 625–653, 1999.
- [SWL11] Bo Shen, Zidong Wang, and Xiaohui Liu. Bounded h_∞ synchronization and state estimation for discrete time-varying stochastic complex for discrete time-varying stochastic complex networks over a finite horizon. 2011.
- [TNXJ17] Hoang-Dung Tran, Luan Viet Nguyen, Weiming Xiang, and Taylor T Johnson. Order-reduction abstractions for safety verification of high-dimensional linear systems. *Discrete Event Dynamic Systems*, 27(2):443–461, 2017.
- [WDZH13] Tong Wang, Yongsheng Ding, Lei Zhang, and Kuangrong Hao. Robust state estimation for discrete-time stochastic genetic regulatory networks with probabilistic measurement delays. *Neurocomputing*, 111:1–12, 2013.

9. APPENDIX

Proof. (Theorem 3.4) According to condition (3.7), $X_b \times X \subseteq \{(x, \hat{x}) \in X \times X \mid \mathcal{B}(x, \hat{x}) \geq \lambda\}$. Then we have

$$\begin{aligned} & \mathbb{P}[x_{av}(k) \in X_b \wedge \hat{x}_{\hat{a}v}(k) \in X \text{ for some } k \in [0, T_d] \mid a, \hat{a}, v] \\ & \leq \mathbb{P}\left[\sup_{0 \leq k \leq T_d} \mathcal{B}(x_{av}(k), \hat{x}_{\hat{a}v}(k)) \geq \lambda \mid a, \hat{a}, v\right] \leq \delta. \end{aligned} \quad (9.1)$$

The proposed bounds in (3.9) follow directly by applying [Kus65, Theorem 3, Chapter III] to the above inequality and employing conditions (3.8) and (3.6), respectively. Inequality (9.1) is obtained by utilizing the result of [Kus67, Theorem 1]. Now we get

$$\begin{aligned} & \mathbb{P}[x_{av}(k) \in X_b \wedge \hat{x}_{\hat{a}v}(k) \in X \text{ for some } k \in [0, T_d] \mid a, \hat{a}, v] \\ & \leq \mathbb{P}[x_{av}(k) \in X_b \text{ for some } k \in [0, T_d] \mid a, v] \\ & \quad + \mathbb{P}[\hat{x}_{\hat{a}v}(k) \in X \text{ for some } k \in [0, T_d] \mid \hat{a}, v] \\ & \quad - \mathbb{P}[x_{av}(k) \in X_b \vee \hat{x}_{\hat{a}v}(k) \in X \text{ for some } k \in [0, T_d] \mid a, \hat{a}, v]. \end{aligned}$$

Since, the second and last terms trivially hold with probability 1, one has

$$\begin{aligned} & \mathbb{P}[x_{av}(k) \in X_b \wedge \hat{x}_{\hat{a}v}(k) \in X \text{ for some } k \in [0, T_d] \mid a, \hat{a}, v] \\ & \leq \mathbb{P}[x_{av}(k) \in X_b \text{ for some } k \in [0, T_d] \mid a, v]. \end{aligned}$$

Now, since the right term of the conjunction (i.e., \wedge) holds for all time, the inequality above becomes an equality and one gets $\mathbb{P}[x_{av}(k) \in X_b \text{ for some } k \in [0, T_d] \mid a, v] \leq \delta$ which concludes the proof. \square

$$\begin{aligned}
& \mathbb{E} \left[\mathcal{B}(f(x(k), v(k), \varsigma_1(k)), \hat{f}(\hat{x}(k), v(k), y(k))) \mid x(k), \hat{x}(k), v(k) \right] \\
&= \mathbb{E} \left[\max_i \left\{ \sigma_i^{-1}(\mathcal{B}_i(f_i(x_i(k), v_i(k), w_i(k), \varsigma_{1_i}(k)), \hat{f}_i(\hat{x}_i(k), v_i(k), \hat{w}_i(k), y_{2_i}(k)))) \mid x(k), \hat{x}(k), v(k), w(k), \hat{w}(k)) \right\} \right] \\
&\leq \max_i \left\{ \sigma_i^{-1}(\mathbb{E} \left[\mathcal{B}_i(f_i(x_i(k), v_i(k), w_i(k), \varsigma_{1_i}(k)), \hat{f}_i(\hat{x}_i(k), v_i(k), \hat{w}_i(k), y_{2_i}(k))) \mid x(k), \hat{x}(k), v(k), w(k), \hat{w}(k)) \right]) \right\} \\
&= \max_i \left\{ \sigma_i^{-1}(\mathbb{E} \left[\mathcal{B}_i(f_i(x_i(k), v_i(k), w_i(k), \varsigma_{1_i}(k)), \hat{f}_i(\hat{x}_i(k), v_i(k), \hat{w}_i(k), y_{2_i}(k))) \mid x_i(k), \hat{x}_i(k), v_i(k), w_i(k), \hat{w}_i(k)) \right]) \right\} \\
&\leq \max_i \left\{ \sigma_i^{-1}(\max\{\bar{\kappa}_i(\mathcal{B}_i(x_i(k), \hat{x}_i(k))), \rho_i(\| \begin{bmatrix} w_i(k) \\ \hat{w}_i(k) \end{bmatrix} \|^2, \bar{\psi}_i)\}) \right\} \\
&= \max_i \left\{ \sigma_i^{-1}(\max\{\bar{\kappa}_i(\mathcal{B}_i(x_i(k), \hat{x}_i(k))), \rho_i(\max_{j,j \neq i} \left\| \begin{bmatrix} w_{ij}(k) \\ \hat{w}_{ij}(k) \end{bmatrix} \right\|^2, \bar{\psi}_i)\}) \right\} \\
&= \max_i \left\{ \sigma_i^{-1}(\max\{\bar{\kappa}_i(\mathcal{B}_i(x_i(k), \hat{x}_i(k))), \rho_i(\max_{j,j \neq i} \left\| \begin{bmatrix} y_{1_{ji}}(k) \\ \hat{y}_{1_{ji}}(k) \end{bmatrix} \right\|^2, \bar{\psi}_i)\}) \right\} \\
&\leq \max_i \left\{ \sigma_i^{-1}(\max\{\bar{\kappa}_i(\mathcal{B}_i(x_i(k), \hat{x}_i(k))), \rho_i(\max_{j,j \neq i} \left\| \begin{bmatrix} h_{1_j}(x_j(k)) \\ h_{1_j}(\hat{x}_j(k)) \end{bmatrix} \right\|^2, \bar{\psi}_i)\}) \right\} \\
&\leq \max_i \left\{ \sigma_i^{-1}(\max\{\bar{\kappa}_i(\mathcal{B}_i(x_i(k), \hat{x}_i(k))), \rho_i(\max_{j,j \neq i} \{\alpha_j^{-1}(\mathcal{B}_j(x_j(k), \hat{x}_j(k)))\}), \bar{\psi}_i)\}) \right\} \\
&= \max_{i,j} \left\{ \sigma_i^{-1}(\max\{\bar{\kappa}_{ij}(\mathcal{B}_i(x_i(k), \hat{x}_i(k))), \bar{\psi}_i\}) \right\} = \max_{i,j} \left\{ \sigma_i^{-1}(\max\{\bar{\kappa}_{ij} \circ \sigma_j \circ \sigma_j^{-1}(\mathcal{B}_j(x_j(k), \hat{x}_j(k))), \bar{\psi}_i\}) \right\} \\
&\leq \max_{i,j,l} \left\{ \sigma_i^{-1}(\max\{\bar{\kappa}_{ij} \circ \sigma_j \circ \sigma_l^{-1}(\mathcal{B}_l(x_l(k), \hat{x}_l(k))), \bar{\psi}_i\}) \right\} \\
&= \max_{i,j} \left\{ \sigma_i^{-1}(\max\{\bar{\kappa}_{ij} \circ \sigma_j(\mathcal{B}(x(k), \hat{x}(k))), \bar{\psi}_i\}) \right\} = \max\{\kappa(\mathcal{B}(x(k), \hat{x}(k))), \bar{\psi}\}. \tag{9.2}
\end{aligned}$$

Proof. (Theorem 3.8) Since ϕ is a stochastic pseudo-simulation function from $\widehat{\Sigma}$ to Σ , one has

$$\begin{aligned}
& \mathbb{P} \left[\sup_{0 \leq k \leq T_d} \|x_{av}(k) - \hat{x}_{av}(k)\| \geq \epsilon \mid a, \hat{a}, v \right] \\
&= \mathbb{P} \left[\sup_{0 \leq k \leq T_d} \varepsilon(\|x_{av}(k) - \hat{x}_{av}(k)\|) \geq \varepsilon(\epsilon) \mid a, \hat{a}, v \right] \\
&\leq \mathbb{P} \left[\sup_{0 \leq k \leq T_d} \phi(x_{av}(k), \hat{x}_{av}(k)) \geq \varepsilon(\epsilon) \mid a, \hat{a}, v \right] \leq \theta.
\end{aligned}$$

The equality holds due to the fact that ε is a \mathcal{K}_∞ function. The second inequality holds based on the first condition of Definition 3.7, and the last inequality follows from the result in [Kus65, Theorem 1]. \square

Proof. (Theorem 5.2) We first show that conditions (3.6) and (3.7) in Definition 3.2 hold. For any $(x, \hat{x}) \in X_a \times X_a$, with $X_a = \prod_{i=1}^N X_{a_i}$, and from (3.3), we have

$$\mathcal{B}(x, \hat{x}) = \max_i \left\{ \sigma_i^{-1}(\mathcal{B}_i(x_i, \hat{x}_i)) \right\} \leq \max_i \left\{ \sigma_i^{-1}(\bar{\gamma}_i) \right\} = \gamma,$$

and simply for any $(x, \hat{x}) \in X_b \times X$, with $X_b = \prod_{i=1}^N X_{b_i}$, $X = \prod_{i=1}^N X_i$ and from (3.4), we have

$$\mathcal{B}(x, \hat{x}) = \max_i \left\{ \sigma_i^{-1}(\mathcal{B}_i(x_i, \hat{x}_i)) \right\} \geq \max_i \left\{ \sigma_i^{-1}(\bar{\lambda}_i) \right\} = \lambda,$$

satisfying conditions (3.3) and (3.4) with $\gamma = \max_i \left\{ \sigma_i^{-1}(\bar{\gamma}_i) \right\}$ and $\lambda = \max_i \left\{ \sigma_i^{-1}(\bar{\lambda}_i) \right\}$. Moreover, $\lambda > \gamma$ according to (5.3). Now we show that condition (3.8) holds, as well. Let $\kappa(s) = \max_{i,j} \left\{ \sigma_j^{-1} \circ \bar{\kappa}_{ij} \circ \sigma_j(s) \right\}$. It follows from (5.2) that $\kappa < \mathcal{I}_d$. Since $\max_i \sigma_i^{-1}$ is concave, one can readily acquire the chain of inequalities in (9.2) using Jensen's inequality. Hence, \mathcal{B} is a CBF for the augmented system $\widehat{\Sigma} = [\Sigma; \widehat{\Sigma}]$, which completes the proof. \square

¹DEPARTMENT OF COMPUTER SCIENCE, LMU MUNICH, GERMANY

Email address: niloofar.jahanshahi@lmu.de

²INSTITUTE FOR DYNAMIC SYSTEMS AND CONTROL, ETH ZURICH, SWITZERLAND

Email address: alavaei@ethz.ch

³DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF COLORADO BOULDER, USA

Email address: majid.zamani@colorado.edu