2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Scalable Distributed Controller Synthesis for Multi-Agent Systems using Barrier Functions and Symbolic Control

David Smith Sundarsingh, Jay Bhagiya, Saharsh, Jeel Chatrola, Adnane Saoud, and Pushpak Jagtap

Abstract— **In this paper, we propose a computationally efficient symbolic controller synthesis technique for multi-agent systems. The paper focuses on synthesizing distributed controllers enforcing local temporal logic specifications along with global safety specifications for multi-agent systems. To solve the problem in a computationally efficient way, we leverage the concept of control barrier functions. In particular, we use a three-step bottom-up approach: first, the symbolic controllers for individual agents are synthesized to enforce local temporal logic specifications, then we use a notion of control barrier functions for symbolic models to compose controlled agent systems by removing unsafe transitions, and finally, we synthesize controller for the reduced composed system to ensure the satisfaction of local temporal logic specifications while ensuring global safety specification. The effectiveness of our approach is demonstrated on a multi-robot system by comparing it with the conventional monolithic symbolic control approaches.**

I. INTRODUCTION

Multi-agent systems (MAS) are made of components operating in the same environment to accomplish their respective tasks. These systems must ensure that each agent accomplishes its task while making sure that it does not violate global safety specifications. For example, a group of drones picking up and dropping packages at designated places in a warehouse while recharging at a common charging point whenever their batteries are low. The drones have to visit various locations in the warehouse while not colliding with each other and no two drones can charge at the same time. Such high-level complex specifications (usually represented using Linear Temporal Logic (LTL)) can be reliably handled by correct-by-construction symbolic control approaches [1] that require state-space and input-space quantization. The need for state space and input-space quantization results in an exponential increase in computational complexity with the dimension of state space in the concrete system, and, hence, these techniques suffer severely from the issue of the so-called curse of dimensionality, especially in the case of systems with high-dimensional state space.

Controller synthesis for MAS is usually done in two ways - top-down and bottom-up approaches. The top-down approach involves the decomposition of global tasks into local ones. For example, [2], [3] decompose global controllers and each agent solves a control problem for the decomposed strategy. The authors in [4] modified this approach by only solving for a sub-group of the MAS, which has mutual specifications. The authors in [5], [6] assign tasks to each agent based on a global specification. These approaches assume that the global specification is decomposable. A similar strategy has been used in [7] using assume-guarantee contracts. On the other hand, bottom-up approaches solve for local specifications with some constraints [8] or synthesize controllers after composing the system from individually controlled agents [9], [10]. While these methods can solve local and global specifications, they require some assumptions on the system [9], [8] or on the specifications [10]. An incremental approach was proposed in [11], where only a subset of agents is incorporated in the synthesis procedure with more agents added until the controller synthesis problem becomes infeasible. This approach only provides probabilistic guarantees. The combination of the two approaches has also been studied. The approach in [12] decomposes the system, solves the local specification, and removes any conflicts after recomposing the system. This process is repeated iteratively without any convergence guarantees.

In the case of MAS, control barrier functions (CBFs) have been used in controller synthesis [13]; however, the control inputs are not bounded and can lead to infeasible input values. The authors in [14] used barrier functions to synthesize a least-intrusive controller limited to collision avoidance. A combination of CBFs and symbolic control has also been studied. The controller in [15] computes a discrete plan and uses CBFs to ensure that the transitions are safe. In [16], the authors generate a discrete plan and use CBFs to execute the plan. Finally, [17], built on [14] by using a nominal controller synthesized in a centralized manner and projecting it onto each agent to satisfy LTL specification on top of collision avoidance. This approach scales badly as centralized controller synthesis is used.

In this paper, we introduce a bottom-up symbolic controller synthesis technique for MAS that is more computationally efficient than the conventional controller synthesis technique. We synthesize the controller in three steps. We first synthesize a controller for each agent in parallel, each ensuring that the controlled agent satisfies the corresponding local specification expressed in Linear Temporal Logic (LTL), using the concept of symbolic control. We then use a notion of control barrier functions (CBFs) defined over the symbolic model that provides safety guarantees for the concrete system to compose the individually controlled agents. These CBFs are used as certificates to remove any unsafe transitions in the composed MAS. The local specifications

*This work was supported in part by the Google Research Grant, the SERB Start-up Research Grant, and the CSR Grants by Siemens and Nokia.

D.S. Sundarsingh, J. Bhagiya, Saharsh, J. Chatrola, and P. Jagtap are with Robert Bosch Centre for Cyber-Physical Systems, IISc, Bangalore, India david_smith_16@outlook.com, pushpak@iisc.ac.in

Adnane Saoud is with College of Computing, University Mohammed VI Polytechnic, Benguerir, Morocco adnane.saoud@um6p.ma

may be violated during this process. Thus, we synthesize a controller for the reduced composed MAS that enforces the local specifications while providing global safety guarantees. We then implement our approach on a MAS for local reach-avoid specification and global safety specification to show the behaviour of the system in a cluttered environment. We also compare our approach with the classical monolithic approach and show its benefits in terms of the computation time required for controller synthesis.

II. Preliminaries and Problem Definition

Notations: For $x \in \mathbb{R}^n$, x_q represents the q^{th} element of the vector $x \in \mathbb{R}^n$, where $q \in \{1, \ldots, n\}$ and the infinity norm of x is $\|x\| := \mathbf{max}_{q \in \{1,\ldots n\}} |x_q|$. For $a, b \in (\mathbb{R} \cup \{-\infty, \infty\})^n$, where $a \leqslant b$ component-wise, the closed hyper-interval is denoted by $[\![a, b]\!] := \mathbb{R}^n \cap ([a_1, b_1] \times \cdots \times [a_n, b_n])$. A relation $R \subseteq A \times B$ can be defined as a map $R : A \to 2^B$ as follows: $b \in R(a)$ iff $(a, b) \in R$. The relation R is strict if $R(a) \neq \varnothing$, $\forall a \in A$. The inverse of the relation is defined as $R^{-1} := \{(b, a) \in B \times A | (a, b) \in R\}$ and can be written as $a \in R^{-1}(b)$. Given a set S, $Int(S)$ and ∂S represent the interior and the boundary of S, respectively. Consider N sets A_i, $i \in \{1, \ldots, N\}$, the Cartesian product of sets is given by $A = \prod_{i \in \{1,\ldots,N\}} A_i := \{(a_1, \ldots, a_N) | a_i \in A_i, i \in \{1, \ldots, N\}\}$. Given N functions $f_i : X_i \to A_i$, the Cartesian product of functions is $f : X \to A := \prod_{i \in \{1,\ldots,N\}} f_i = (f_1(x_1), \ldots, f_N(x_N))$. The composition of two maps H and R is $H \circ R(x) := H(R(x))$. A function $\alpha : \mathbb{R}_0^+ \to \mathbb{R}_0^+$ is of class $\mathcal{K}$ if $\alpha(0) = 0$, and it is strictly increasing. If $\alpha \in \mathcal{K}$ is unbounded, it is of class $\mathcal{K}_\infty$.

A. Discrete-time Multi-Agent Systems

Consider a collection of $N \in \mathbb{N}$ agents and let $I = \{1, \ldots, N\}$. Each agent's state evolution is given by the following discrete-time control system:

$$\mathsf{x}_i(k+1) = \mathsf{f}_i(\mathsf{x}_i(k), \mathsf{u}_i(k)), \ i \in I, \ k \in \mathbb{N}_0, \qquad (1)$$

where $\mathsf{x}_i(k) \in X_i \subset \mathbb{R}^{n_i}$ is the state of the i^{th} agent and $\mathsf{u}_i(k) \in U_i \subset \mathbb{R}^{m_i}$ is the input to the agent.
The state evolution of the multi-agent system is given by:

$$\mathsf{x}(k+1) = \mathsf{f}(\mathsf{x}(k), \mathsf{u}(k)), \ k \in \mathbb{N}_0, \ x(0) \in X^0, \qquad (2)$$

where X^0 is the set of initial states, $\mathsf{x}(k) \in X := \Pi_{i \in I} X_i \subset \mathbb{R}^n$ is the state of the multi-agent system, $n = \Sigma_{i \in I} n_i$, $\mathsf{u}(k) \in U := \Pi_{i \in I} U_i \subset \mathbb{R}^m$ is the input to the system and $m = \Sigma_{i \in I} m_i$. The function f is given by $\mathsf{f} : X \times U \to X$ and $\mathsf{f}(\mathsf{x}(k), \mathsf{u}(k)) := \Pi_{i \in I} \mathsf{f}_\mathsf{i}(\mathsf{x}_\mathsf{i}(k), \mathsf{u}_\mathsf{i}(k))$. The trajectory of system (2) starting from a state $x \in X^0$ under the input signal u is given by $\mathsf{x}_{x\mathsf{u}}$ and $\mathsf{x}_{x\mathsf{u}}(k)$ gives the value of the state of the system at sampling instance k.

The reachable set of system (2) from a set $\mathcal{X} \subseteq X$ under an input $u \in U$ is given by $Reach(\mathcal{X}, u) := \bigcup_{x \in \mathcal{X}} \mathsf{f}(x, u)$, which is the set of all states that the system "reaches" when an input u is applied at all the states in $\mathcal{X}$ in a one-time step. This reachable set is difficult to compute, so we use the over-approximated reachable set, $\overline{Reach}(x, u)$. Several approaches are available in the literature for computing this over-approximated set; for example, [18], [19] and [20].

B. Transition Systems

We now introduce the notion of transition systems [1] which will serve as a unified representation for discrete-time control systems and their corresponding symbolic models.

Definition 2.1: A transition system is a tuple $\Sigma = (X, X^0, U, F)$, where X is the set of states (possibly infinite), $X^0 \subseteq X$ is the set of initial states, U is the set of inputs (possibly infinite), and the map $F : X \times U \rightrightarrows X$ is the transition relation.
The set of admissible inputs for $x \in X$ is denoted by $U^a(x) := \{u \in U \mid F(x, u) \neq \varnothing\}$. We use $x' \in F(x, u)$ to represent the u-successor of state x.
Consider the discrete-time control system of agent i as given in (1). The transition system representation of the i^{th} agent is given by the tuple $\Sigma_i = (X_i, X_i^0, U_i, F_i)$, where $X_i \subset \mathbb{R}^{n_i}$ is the set of the states of agent i, $X_i^0 \subseteq X_i$ is the set of initial states, $U_i \subset \mathbb{R}^{m_i}$ is the set of inputs for agent i and for $x_i \in X_i$, $u_i \in U_i$, $F_i(x_i, u_i) := \mathsf{f}_i(x_i, u_i)$.
The composition of the N transition systems, which represents the multi-agent system (2) is given by definition below.

Definition 2.2: Given a collection of $N \in \mathbb{N}$ agents represented as $\{\Sigma_i\}_{i \in I}$, where $I = \{1, \ldots, N\}$, the composed transition system is $\Sigma = \left(X, X^0, U, F\right)$, where

- $X = \prod_{i \in I} X_i$, $X^0 \subseteq X$, $U = \prod_{i \in I} U_i$,
- for $x \in X$ and $u \in U$, $F(x, u) = \prod_{i \in I} F_i(x_i, u_i)$.

C. Problem Formulation

Next, we formally state the problem considered here:

Problem 2.3: Given N agents with dynamics as in (1), local specifications ψ_i expressed as LTL formulas [21] for each agent and global safety specification Φ over the MAS (2); design a controller for the MAS that enforces global safety specification and the local LTL specifications.

One can solve Problem 2.3 for a MAS monolithically using symbolic control techniques (as discussed in Section III) for satisfying the global and local specifications $\varphi = \Psi \wedge \Phi$, where $\Psi = \bigwedge_{i \in I} \psi_i$, but scalability and computational efficiency are stringent issues for controller synthesis.

To deal with the scalability issue and, as a consequence, to reduce computational complexity, we propose to use a bottom-up approach consisting of three steps:

1) We construct a symbolic controller for each of the N agents Σ_i to satisfy the corresponding local LTL specification ψ_i, where $i \in \{1, \ldots, N\}$, as explained in Section III. Using the symbolic controller, we construct the individual controlled agents.
2) For the composed controlled MAS, resulting from the composition of the controlled agents obtained in step (1), we construct a barrier function [22] that enforces the global safety specification Φ. We use a notion of barrier functions (introduced in Section IV) as certificates to remove transitions that violate the safety specification in the composed system.
3) Since the local specifications may be violated due to the safety-enforcing barrier functions, we synthesize a controller for the controlled system obtained in step (2) to achieve the specification $\Psi = \bigwedge_{i \in I} \psi_i$.

The proposed controller ensures that the MAS satisfies the local specification Ψ and the global specification Φ.

III. Symbolic Control

In this section, we will briefly discuss symbolic control and how it can be used to synthesize controllers to satisfy a given specification. In order to relate the discrete-time control system and its symbolic model, we use the notion of feedback refinement relation [20].

A. Feedback Refinement Relation

Definition 3.1: Consider two transition systems $\Sigma = (X, X^0, U, F)$ and $\hat{\Sigma} = (\hat{X}, \hat{X}^0, \hat{U}, \hat{F})$. A strict relation $Q \subseteq X \times \hat{X}$ is said to be a feedback refinement relation from Σ to $\hat{\Sigma}$, denoted by $\Sigma \preceq_Q \hat{\Sigma}$, if for each $(x, \hat{x}) \in Q$ the following conditions hold:

- $\hat{U}^a(\hat{x}) \subseteq U^a(x)$,
- $u \in \hat{U}^a(\hat{x}) \implies Q(F(x,u)) \subseteq \hat{F}(\hat{x}, u)$.

The feedback refinement relation Q allows to transform a controller for the abstraction $\hat{\Sigma}$ into a controller for the original system Σ.

B. Construction of Symbolic Models

In order to synthesize controllers for the concrete system Σ, we need to construct its symbolic model $\hat{\Sigma}$, which is related to the original system Σ through the feedback refinement relation.

Definition 3.2: The symbolic model of the system Σ is given by $\hat{\Sigma} = (\hat{X}, \hat{X}^0, \hat{U}, \hat{F})$, where

- $\hat{X}$ is a cover over X whose elements are closed hyper-intervals called cells. Let $\bar{\hat{X}} \subseteq \hat{X}$ be a compact set of congruent hyper-rectangles aligned on a uniform grid parameterized with a quantization parameter $\eta \in (\mathbb{R}^+)^n$. Each $\hat{x} \in \bar{\hat{X}}$ is given by $c_{\hat{x}} + \llbracket -\frac{\eta}{2}, \frac{\eta}{2} \rrbracket$, where $c_{\hat{x}} \in \eta\mathbb{Z}^n$ and $\eta\mathbb{Z}^n = \{c \in \mathbb{R}^n | \exists_{l \in \mathbb{Z}^n} \forall_{q \in \{1,\ldots,n\}} c_q = l_q \eta_q\}$. The cells in $\hat{X} \backslash \bar{\hat{X}}$ are called overflow cells,
- $\hat{X}^0 = \hat{X} \cap X^0$ and $\hat{U}$ is a finite subset of U,
- for $\hat{x} \in \bar{\hat{X}}$ and $\hat{u} \in \hat{U}$, a set $A := \{\hat{x}' \in \hat{X} | \hat{x}' \cap \overline{Reach}(\hat{x}, \hat{u}) \neq \varnothing\}$. If $A \subseteq \bar{\hat{X}}$ and $\hat{x}' \notin \hat{X} \backslash \bar{\hat{X}}$, $\forall \hat{x}' \in A$ then $\hat{F}(\hat{x}, \hat{u}) = A$.

For a detailed procedure on constructing the symbolic model, kindly refer to [23].

Theorem 3.3: [20, Theorem VIII.4] If $\hat{\Sigma}$ is the symbolic model of Σ constructed according to Definition 3.2 then the relation $Q \subseteq X \times \hat{X}$ defined by $= \{(x, \hat{x}) \in X \times \hat{X} : x \in \hat{x}\}$ is feedback refinement relation from Σ to $\hat{\Sigma}$.

C. Controller Synthesis using Symbolic Models

Consider the transition system $\Sigma = (X, X^0, U, F)$ and a memoryless controller $C : X \rightrightarrows U$, where for all $x \in X$, $C(x) \subseteq U^a(x)$. Let the domain of the controller be $dom(C) := \{x \in X | C(x) \neq \varnothing\}$.

Definition 3.4: Given a controller C and a transition system Σ, the controlled system is given by the tuple $\Sigma|C = (X_C, X_C^0, U_C, F_C)$, where

- $X_C = X \cap dom(C)$, $X_C^0 \subseteq X_C$, $U_C = U$,
- for $x_C \in X_C$ and $u_C \in U_C$, $x'_C \in F_C(x_C, u_C)$ iff $x'_C \in F(x_C, u_C)$ and $u_C \in C(x_C)$.

Let P be the set of atomic propositions that labels the states in $X \subset \mathbb{R}^n$ through a labelling function $\mathcal{L} : X \to 2^P$ and φ be an LTL specification over P. The control inputs u applied to the system according to C generates a trajectory $\mathsf{x}_{x\mathsf{u}}$ from the initial state x. We say that the system $\Sigma|C \models \varphi$ if $\mathcal{L}(\mathsf{x}_{x\mathsf{u}}) \models \varphi$. For more information on specification satisfaction, refer [20, Definition VI.1].

Given the symbolic model $\hat{\Sigma}$ and the relation $Q \subseteq X \times \hat{X}$, we first synthesize a controller $\hat{C}$ such that $\hat{\Sigma}|\hat{C} \models \hat{\varphi}$ using graph theoretical approaches [1], where $\hat{\varphi}$ is the symbolic specification associated with Σ, $\hat{\Sigma}$, Q and φ such that, if $\mathcal{L}(\hat{x}) \subseteq \hat{\varphi}$ and $(x, \hat{x}) \in Q$, then $\mathcal{L}(x) \subseteq \varphi$.

Theorem 3.5: [20, Theorem VI.3] If $\Sigma \preceq_Q \hat{\Sigma}$ and $\hat{C}$ is the symbolic controller such that $\hat{\Sigma}|\hat{C} \models \hat{\varphi}$, then $\Sigma|C \models \varphi$, where $C := \hat{C} \circ Q$.

The controller $\hat{C}$, synthesized for symbolic model $\hat{\Sigma}$ satisfying global and local specifications, defined in Problem 2.3, can be refined for the concrete system Σ with the help of relation Q. The controlled system $\Sigma|C \models \varphi$, where $\varphi := \Psi \wedge \Phi$ is the combination of local and global specifications. Many toolboxes are available for symbolic controller synthesis, for example, [23], [24] and [25]. For scalability, we first synthesize a controller that satisfies the local specification ψ_i for the i^{th} local symbolic model (i^{th} agent) with $\Psi = \bigwedge_{i \in I} \psi_i$ and enforce global safety specification Φ on the composed symbolic model with the notion of control barrier functions, discussed in the next section.

IV. Barrier Certificate for Symbolic Models

To deal with global safety specification Φ, we leverage the concept of control barrier function [26]. Consider a discrete-time system as defined in (2). Let the safe set $S \subseteq X \subset \mathbb{R}^n$ be defined as the superlevel set of a continuous function $B : \mathbb{R}^n \to \mathbb{R}$ and is given by:

$$S = \{x \in X | B(x) \geqslant 0\}, \tag{3}$$
$$Int(S) = \{x \in X | B(x) > 0\}, \tag{4}$$
$$\partial S = \{x \in X | B(x) = 0\}. \tag{5}$$

Definition 4.1: Given the transition system $\Sigma = (X, X^0, U, F)$ in Definition 2.1 and a set $S \subseteq X$. The set S is said to be controlled invariant for the transition system Σ if for all $x \in S$, there exists $u \in U$ satisfying $F(x, u) \subseteq S$.

Theorem 4.2: [26, Lemma 1] Given the discrete-time control system (2) and a safe set $S \subseteq X \subset \mathbb{R}^n$ as defined in (3)-(5) as a superlevel set of a continuous function $B : \mathbb{R}^n \to \mathbb{R}$. The set S is is a controlled invariant for the system in (2) if there exists a $\mathcal{K}_\infty$ map α, satisfying $\alpha(r) < r$, for all $r > 0$ and such that the following holds: for all $x \in X$, there exists $u \in U$ satisfying

$$B(\mathsf{f}(x, u)) - B(x) \geqslant -\alpha(B(x)). \tag{6}$$

To solve Problem 2.3 in a scalable way, we first define a symbolic safe set $\hat{S}$ that is compatible with the symbolic model using barrier function B (3)-(6) defining safe set S for the original system (2). For this, we need the following assumption over function $B : X \to \mathbb{R}$.

Assumption 4.3: The barrier functions $B : X \to \mathbb{R}$ defined in Theorem 4.2 satisfy the global Lipschitz continuity condition: there exists a constant $\mathcal{L}^x \in \mathbb{R}_0^+$ such that $\|B(x) - B(y)\| \leqslant \mathcal{L}^x \|x - y\|$ for all $x, y \in X$.

Given Assumption 4.3 and a symbolic model $\hat{\Sigma} = (\hat{X}, \hat{X}^0, \hat{U}, \hat{F})$ with a symbolic state given by $\hat{x} := c_{\hat{x}} + \llbracket -\frac{\eta}{2}, \frac{\eta}{2} \rrbracket \in \hat{X}$ and state space discretization $\eta = (\eta_1, \ldots, \eta_n) \in (\mathbb{R}^+)^n$ as defined in Definition 3.2, we define a symbolic safe set $\hat{S}$ using barrier function B in Theorem 4.2 as:

$$\hat{S} = \{\hat{x} \in \hat{X} | B(c_{\hat{x}}) - \mathcal{L}^x \frac{\eta_{max}}{2} \geqslant 0\} \tag{7}$$

$$Int(\hat{S}) = \{\hat{x} \in \hat{X} | B(c_{\hat{x}}) - \mathcal{L}^x \frac{\eta_{max}}{2} > 0\} \tag{8}$$

$$\partial \hat{S} = \{\hat{x} \in \hat{X} | B(c_{\hat{x}}) - \mathcal{L}^x \frac{\eta_{max}}{2} = 0\}, \tag{9}$$

where $\eta_{max} = \mathbf{max}_{j \in \{1,\ldots,n\}} \eta_j$.

Theorem 4.4: Consider a system $\Sigma = (X, X^0, U, F)$, its symbolic model $\hat{\Sigma} = (\hat{X}, \hat{X}^0, \hat{U}, \hat{F})$ constructed with relation $Q \subseteq X \times \hat{X}$ and state space quantization $\eta \in (\mathbb{R}^+)^n$ as defined in Definition 3.2, a safe set S as defined in (3)-(5), and the symbolic safe set $\hat{S}$ as defined in (7)-(9). If for all $\hat{x} \in \hat{S}$, there exists $\hat{u} \in \hat{U}^a(\hat{x})$ such that

$$\mathbf{min}_{\hat{\mathbf{x}}' \in \hat{\mathbf{F}}(\hat{\mathbf{x}}, \hat{\mathbf{u}})} [B(c_{\hat{x}'}) - B(c_{\hat{x}})] \geqslant -\alpha(B(c_{\hat{x}}) - \mathcal{L}^x \frac{\eta_{max}}{2}),$$

where $B : X \to \mathbb{R}$ and $\alpha \in \mathcal{K}_\infty$ are defined in Theorem 4.2, then $Q^{-1}(\hat{S}) \subset S$ and $\hat{S}$ is invariant for system $\hat{\Sigma}$.

Proof: Let us first show that $Q^{-1}(\hat{S}) \subset S$.
From Definition 3.2, we have $\hat{x} := c_{\hat{x}} + \llbracket \frac{-\eta}{2}, \frac{\eta}{2} \rrbracket \in \hat{X}$ and using the fact $\eta_{max} = \mathbf{max}_{j \in \{1,\ldots,n\}} \eta_j$, one obtains for all $(x, \hat{x}) \in Q$, $\|c_{\hat{x}} - x\| \leqslant \frac{\eta_{max}}{2}$. Using Lipschitz continuity of B, $\forall (x, \hat{x}) \in Q$, we get

$$B(c_{\hat{x}}) - B(x) \leqslant \|B(c_{\hat{x}}) - B(x)\| \leqslant \mathcal{L}^x \|c_{\hat{x}} - x\| \leqslant \mathcal{L}^x \frac{\eta_{max}}{2},$$

where $\mathcal{L}^x$ is the Lipschitz constant of the function B. Thus,

$$\forall (x, \hat{x}) \in Q, \; B(c_{\hat{x}}) - \mathcal{L}^x \frac{\eta_{max}}{2} \leqslant B(x). \tag{10}$$

Thus, $B(c_{\hat{x}}) - \mathcal{L}^x \frac{\eta_{max}}{2} \geqslant 0 \implies B(x) \geqslant 0$, i.e., for all $\hat{x} \in \hat{S}$, $Q^{-1}(\hat{x}) \subset S$. Thus we have $Q^{-1}(\hat{S}) \subset S$.
Now to show that $\hat{S}$ is invariant for $\hat{\Sigma}$, we have that for all $\hat{x} \in \hat{S}$ there exists $\hat{u} \in \hat{U}^a(\hat{x})$ such that

$$\begin{aligned} &\mathbf{min}_{\hat{\mathbf{x}}' \in \hat{\mathbf{F}}(\hat{\mathbf{x}}, \hat{\mathbf{u}})} [B(c_{\hat{x}'}) - B(c_{\hat{x}})] \\ &= \mathbf{min}_{\hat{\mathbf{x}}' \in \hat{\mathbf{F}}(\hat{\mathbf{x}}, \hat{\mathbf{u}})} [B(c_{\hat{x}'}) - \mathcal{L}^x \frac{\eta_{max}}{2} - B(c_{\hat{x}}) + \mathcal{L}^x \frac{\eta_{max}}{2}] \\ &\geqslant -\alpha(B(c_{\hat{x}}) - \mathcal{L}^x \frac{\eta_{max}}{2}). \end{aligned}$$

Thus one has for all $\hat{x} \in \hat{S}$ there exists $\hat{u} \in \hat{U}^a(\hat{x})$ such that

$$B(c_{\hat{x}'}) - \mathcal{L}^x \frac{\eta_{max}}{2} - B(c_{\hat{x}}) + \mathcal{L}^x \frac{\eta_{max}}{2} \geqslant -\alpha(B(c_{\hat{x}}) - \mathcal{L}^x \frac{\eta_{max}}{2}),$$

which implies that

$$B(c_{\hat{x}'}) - \mathcal{L}^x \frac{\eta_{max}}{2} \geqslant (I_d - \alpha) \circ (B(c_{\hat{x}}) - \mathcal{L}^x \frac{\eta_{max}}{2})$$

for all $\hat{x}' \in \hat{F}(\hat{x}, \hat{u})$. Since $\alpha \in \mathcal{K}_\infty$ one has that $(I_d - \alpha) \in \mathcal{K}_\infty$ which implies from condition (7) (i.e., $B(c_{\hat{x}}) - \mathcal{L}^x \frac{\eta_{max}}{2} \geqslant 0$ for all $\hat{x} \in \hat{S}$) that for all $\hat{x} \in \hat{S}$ we have $B(c_{\hat{x}'}) - \mathcal{L}^x \frac{\eta_{max}}{2} \geqslant 0 \implies \hat{x}' \in \hat{S}$, $\forall \hat{x}' \in \hat{F}(\hat{x}, \hat{u})$. This proves the invariance of the set $\hat{S}$. ■

Remark 4.5: Since we know that $Q^{-1}(\hat{S}) \subset S$ (from Theorem 4.4) and with $\hat{S}$ as invariant, the system does not violate the safety specification Φ by staying inside S.

V. Scalable Controller Synthesis for Multi-Agent Systems

A. Controller Synthesis for Each Agent (Symbolic Model)

Consider the problem of controller synthesis for each agent (1) represented by the transition system $\Sigma_i = (X_i, X_i^0, U_i, F_i)$ given a local LTL specification ψ_i. Using symbolic control, we first construct the symbolic model of each agent Σ_i given by $\hat{\Sigma}_i = (\hat{X}_i, \hat{X}_i^0, \hat{U}_i, \hat{F}_i)$ (as discussed in Section III-B) such that $\Sigma_i \preceq_{Q_i} \hat{\Sigma}_i$, where $Q_i \subseteq X_i \times \hat{X}_i$ is the strict feedback refinement relation. We then synthesize a controller $\hat{C}_i$ such that $\hat{\Sigma}_i | \hat{C}_i \models \hat{\psi}_i$, where $\hat{\psi}_i$ is the symbolic specification for $\hat{\Sigma}_i$ (related to ψ_i, Σ_i and Q_i). Theorem 3.5 shows that we can refine the controller $\hat{C}_i$ using the feedback refinement relation Q_i and the refined controller $C_i := \hat{C}_i \circ Q_i$ is such that $\Sigma_i | C_i \models \psi_i$.

After controller synthesis, we obtain the controlled agents $\hat{\Sigma}_i | \hat{C}_i = (\hat{X}_{C_i}, \hat{X}_{C_i}^0, \hat{U}_{C_i}, \hat{F}_{C_i})$, $i \in \{1, 2, \ldots, N\}$, as shown in Definition 3.4, where $\hat{X}_{C_i} = \hat{X}_i \cap dom(\hat{C}_i)$, $\hat{X}_{C_i}^0 \subseteq \hat{X}_{C_i}$, $\hat{U}_{C_i} = \hat{U}_i$ and for $\hat{x} \in \hat{X}_{C_i}$, $\hat{u} \in \hat{U}_{C_i}$, $\hat{x}' \in \hat{F}_{C_i}(\hat{x}, \hat{u})$ iff $\hat{x}' \in \hat{F}_i(\hat{x}, \hat{u})$ and $\hat{u} \in \hat{C}_i(\hat{x})$.

B. Construction of the Composed System using Control Barrier Certificates

We will now compose the individual symbolic models of the controlled systems of each agent.

Given a collection of N $(\in \mathbb{N})$ controlled systems where each controlled system is given by $\hat{\Sigma}_i | \hat{C}_i = (\hat{X}_{C_i}, \hat{X}_{C_i}^0, \hat{U}_{C_i}, \hat{F}_{C_i})$ and $I = \{1, \ldots, N\}$, the composed controlled system is given by $\hat{\Sigma} | \hat{C} = (\hat{X}_C, \hat{X}_C^0, \hat{U}_C, \hat{F}_C)$ constructed based on Definition 2.2, where $\hat{X}_C = \prod_{i \in I} \hat{X}_{C_i}$, $\hat{X}_{C_i}^0 \subseteq \hat{X}_C$, $\hat{U}_C = \prod_{i \in I} \hat{U}_{C_i}$ and for $\hat{x} \in \hat{X}_C$ and $\hat{u} \in \hat{U}_C$, $\hat{F}_C(\hat{x}, \hat{u}) = \prod_{i \in I} \hat{F}_{C_i}(\hat{x}, \hat{u})$.

Definition 5.1: Let $B : X \to \mathbb{R}$ be the CBF that enforces the safety specification Φ. We construct the safety controller $\hat{C}_S$ for the system $\hat{\Sigma} | \hat{C}$ defined above, as follows:

- $\hat{C}_S(\hat{x}) = \hat{U}_C^a(\hat{x}) \cap \{\hat{u} | \mathbf{min}_{\hat{\mathbf{x}}' \in \hat{\mathbf{F}}(\hat{\mathbf{x}}, \hat{\mathbf{u}})} [B(c_{\hat{x}'}) - B(c_{\hat{x}})] \geqslant -\alpha(B(c_{\hat{x}}) - \mathcal{L}^x \frac{\eta_{max}}{2})\}$ and
- $dom(\hat{C}_S) \subseteq X_C \cap \hat{S}$.

We can now construct a controlled system $(\hat{\Sigma} | \hat{C}) | \hat{C}_S = (\hat{X}_S, \hat{X}_S^0, \hat{U}_S, \hat{F}_S)$ as defined in Definition 3.4, where $\hat{X}_S = \hat{X}_C \cap dom(\hat{C}_S)$, $\hat{X}_S^0 \subseteq \hat{X}_S$, $\hat{U}_S = \hat{U}_C$ and for $\hat{x} \in \hat{X}_S$ and $\hat{u} \in \hat{U}_S$, $\hat{x}' \in \hat{F}_S(\hat{x}, \hat{u})$ iff $\hat{x}' \in \hat{F}_C(\hat{x}, \hat{u})$ and $\hat{u} \in \hat{C}_S(\hat{x})$.

Remark 5.2: Note that only the transitions that lead back to the set $\hat{S}$ are included in the transition system $(\hat{\Sigma} | \hat{C}) | \hat{C}_S$.

At some $\hat{x} \in \hat{X}_S$, $\hat{U}^a_S(\hat{x})$ may be empty because there could be no inputs in $\prod_{i\in I} \hat{U}^a_{C_i}(\hat{x}_i)$ that brings the system to $\hat{S}$.

To restore the local specifications (violated due to the safety-enforcing barrier certificate), it is necessary to synthesize a controller $\hat{C}_B$ for the composed symbolic model's specification given by $\hat{\Psi} = \Pi_{i\in I}\hat{\psi}_i$.

The following result shows that the combination of the controllers C_B, C_S and C_i, $i \in \{1, 2, \ldots, N\}$, designed before makes it possible for the discrete-time control system in (2) to satisfy the control objective defined in Problem 2.3.

Theorem 5.3: Given the controlled agents $\hat{\Sigma}_i|\hat{C}_i$ with $i \in I = \{1, \ldots, N\}$, the strict relation $Q_i \subseteq X_i \times \hat{X}_i$, LTL specification $\Psi := \bigwedge_{i\in I} \psi_i$, symbolic specification $\hat{\Psi}$ resulting from the concrete specification Ψ, the symbolic safe set $\hat{S}$ defined in (7)-(9) and the safe set S defined in (3)-(5), if $\hat{C}_B$ is a controller such that $((\hat{\Sigma}|\hat{C})|\hat{C}_S)|\hat{C}_B \models \hat{\Psi}$ then, $((\Sigma|C)|C_S)|C_B \models \Psi$, where $C_B := \hat{C}_B \circ Q$ and the trajectories of the controlled MAS $((\Sigma|C)|C_S)|C_B$ stays inside the safe set S.

Proof: From [20, Theorem VI.3] and [20, Corollary VI.5], we know that $\Sigma_i|C_i \preceq_{Q_i} \hat{\Sigma}_i|\hat{C}_i$ since $\Sigma_i \preceq_{Q_i} \hat{\Sigma}_i$ by construction and $C_i := \hat{C}_i \circ Q_i$.

By composing the controlled agents and since there is no coupling between the agents, one gets $\Sigma|C \preceq_Q \hat{\Sigma}|\hat{C}$, where Σ is the MAS resulting from the composition of the agents Σ_i, $i \in \{1, \ldots, N\}$, $\hat{\Sigma}$ is the transition system resulting from the composition of the local abstractions $\hat{\Sigma}_i$, $i \in \{1, \ldots, N\}$. The set of states for the composed MAS and the composed local abstractions are given by $X := \prod_{i\in I} X_i$ and $\hat{X} := \prod_{i\in I} \hat{X}_i$, respectively. The controller $C : X \rightrightarrows U$ is defined for $x = (x_1, \ldots, x_N) \in X$ as $u = (u_1, \ldots, u_N) \in C(x)$ if and only if $u_i \in C_i(x_i)$, for all $i \in \{1, \ldots, N\}$. Similarly the abstract controller $\hat{C} : \hat{X} \rightrightarrows \hat{U}$ is defined for $\hat{x} = (\hat{x}_1, \ldots, \hat{x}_N) \in \hat{X}$ as $\hat{u} = (\hat{u}_1, \ldots, \hat{u}_N) \in \hat{C}(\hat{x})$ if and only if $\hat{u}_i \in \hat{C}_i(\hat{x}_i)$, for all $i \in \{1, \ldots, N\}$. The feedback refinement relation $Q \subseteq X \times \hat{X}$ is defined as $Q = \{(x, \hat{x}) \in X \times \hat{X} \mid (x_i, \hat{x}_i) \in Q_i, \quad i \in \{1, \ldots, N\}\}$. We synthesize a safety controller $\hat{C}_S$ as given in Definition 5.1 for the system $\hat{\Sigma}|\hat{C}$. By construction, this controller ensures that the controlled system $(\hat{\Sigma}|\hat{C})|\hat{C}_S$ never leaves $\hat{S}$. The refined controller $C_S := \hat{C}_S \circ Q$ is such that, $(\Sigma|C)|C_S \preceq_Q (\hat{\Sigma}|\hat{C})|\hat{C}_S$ since $\Sigma|C \preceq_Q \hat{\Sigma}|\hat{C}$.

We now synthesize a controller $\hat{C}_B$ such that $((\hat{\Sigma}|\hat{C})|\hat{C}_S)|\hat{C}_B \models \hat{\Psi}$ and since $(\Sigma|C)|C_S \preceq_Q (\hat{\Sigma}|\hat{C})|\hat{C}_S$, $C_B := \hat{C}_B \circ Q$ is the refined controller such that $((\Sigma|C)|C_S)|C_B \models \Psi$ due to Theorem 3.5.

With the composed controlled system we have,

$$((\Sigma|C)|C_S)|C_B \preceq_Q ((\hat{\Sigma}|\hat{C})|\hat{C}_S)|\hat{C}_B. \tag{11}$$

Since $\hat{C}_B(\hat{x}) \subseteq \hat{U}_S(\hat{x})$ and $dom(\hat{C}_B) \subseteq \hat{X}_S$, all trajectories of the system $((\hat{\Sigma}|\hat{C})|\hat{C}_S)|\hat{C}_B$ evolve within the set $\hat{S}$. From (11), it is clear that $((\Sigma|C)|C_S)|C_B$ will also remain in $\hat{S}$, which implies from Theorem 4.4 that the system $((\Sigma|C)|C_S)|C_B$ always remains in S. Hence, the combination of refined controllers C, C_S and C_B allows to satisfy the specifications defined in Problem 2.3. ■

TABLE I: Computation time comparison

Number of	Computation Time (secs)		
Robots	Monolithic	Proposed	Percent reduction
2	170.24	32.11	81.25
3	>4 weeks	85985.05	>96.5

VI. Experimental Results

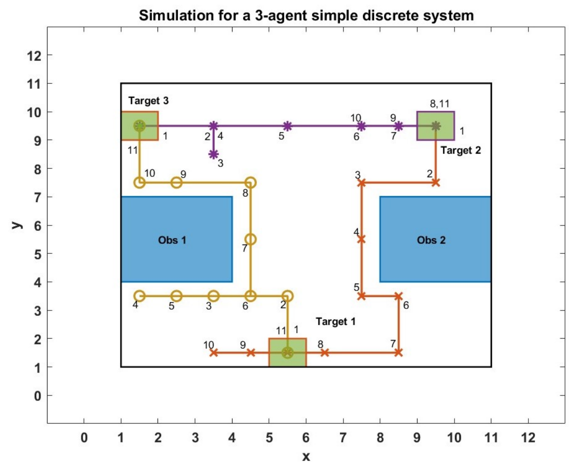

Fig. 1: Simulation for a multi-agent system with three agents

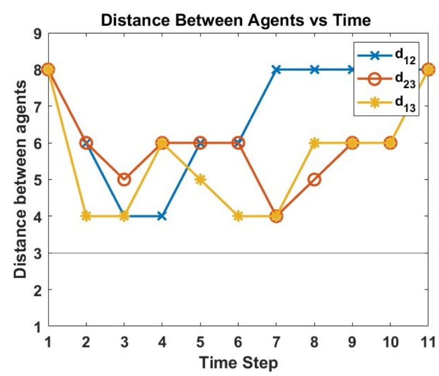

Fig. 2: Distance between two agents for MAS with Three Agents. The grey line is lower bound on the safe distance.

We compare the proposed approach with a centralized controller synthesis technique. We simulate a discrete system where each agent is given by

$$\mathsf{x}_i(k+1) = \mathsf{x}_i(k) + \mathsf{u}_i(k), \; i \in \{1, \ldots, N\}, \; k \in \mathbb{N}_0,$$

where $\mathsf{x}_i(k) \in X = [0, 10] \times [0, 10] \subset \mathbb{R}^2$ is the state of the system and $\mathsf{u}_i(k) \in U = \{(-2, 0), (-1, 0), (1, 0), (2, 0), (0, -2), (0, -1), (0, 1), (0, 2)\} \subset \mathbb{R}^2$ is the input to the system. We ran two experiments with $N = 2$ and $N = 3$. The global safety specification is given by a set of pair-wise CBFs as

$$B_{ij}(x) = \|x^i - x^j\| - d_{ij}, \; \forall i, j \in N \text{ and } i \neq j, \tag{12}$$

where $d_{ij} = 3$ is the distance between the agents i and j. The local LTL specification for agent i is given by

$\psi_i = \Diamond Target_i \wedge (\Box\neg(Obs_1 \vee Obs_2))$, where $Target_i$ is the target of agent i, Obs_1 and Obs_2 are the obstacles in the state-space, $\Box$ and $\Diamond$ represent temporal operators always and eventually, respectively. We used a computer with AMD Ryzen 9 5950x, 128 GB RAM, and NVIDIA RTX 3080Ti graphics card to perform simulations that were run on MATLAB. The state quantization parameter is $\eta = [1, 1]$.

Table I shows the synthesis time of the proposed technique compared to that of the monolithic approach. For the 2 agent example, the proposed technique took 32.082 secs for controller synthesis, an 81.25% reduction compared to the monolithic approach that took 170.2421 secs. For 3 agents, the proposed technique took 85985.05 secs for synthesis, while the monolithic approach did not finish synthesizing within 4 weeks, raising the reduction in time to more than 96.5%. The proposed technique gets progressively faster compared to the monolithic approach with increased state-space dimensions.

Figure 1 shows the simulation of a three-agent system with a local specification of avoiding the obstacles, Obs 1 and Obs 2, and reaching the corresponding targets while ensuring the global safety specification. One can see that the MAS satisfies both local and global specifications. The orange line shows the trajectory of agent 1; the purple line shows the trajectory of agent 2; and the yellow line shows the trajectory of agent 3. Figure 2 shows the distance between the agents as they move in the arena. The grey horizontal line shows the lower bound on the distance between agents. The graph clearly shows that all three agents never get closer than three units to each other, thereby satisfying the global safety specification.

VII. Conclusion

We proposed a three-step bottom-up symbolic approach for MAS by combining symbolic control and CBFs. We have also provided a symbolic safe set defined over the symbolic model that provides safety guarantees for the concrete system and have used this notion of barrier functions to enforce global safety specifications. We have proven the correctness of our approach and have formally shown that the final controlled multi-agent system satisfies both local and global specifications. The experimental results show the benefits of the proposed approach in terms of computation time.

References

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

[2] R. Majumdar, K. Mallik, M. Salamati, S. Soudjani, and M. Zareian, "Symbolic reach-avoid control of multi-agent systems," in *Proceedings of the ACM/IEEE 12th International Conference on Cyber-Physical Systems*, pp. 209–220, 2021.

[3] J. Dai and H. Lin, "Automatic synthesis of cooperative multi-agent systems," in *53rd IEEE Conference on Decision and Control*, pp. 6173–6178, 2014.

[4] A. Nikou, J. Tumova, and D. V. Dimarogonas, "Probabilistic plan synthesis for coupled multi-agent systems.," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 10766–10771, 2017. 20th IFAC World Congress.

[5] P. Schillinger, M. Bürger, and D. V. Dimarogonas, "Auctioning over probabilistic options for temporal logic-based multi-robot cooperation under uncertainty," in *IEEE International Conference on Robotics and Automation (ICRA)*, pp. 7330–7337, 2018.

[6] J. Chen, R. Sun, and H. Kress-Gazit, "Distributed control of robotic swarms from reactive high-level specifications," in *IEEE 17th International Conference on Automation Science and Engineering (CASE)*, pp. 1247–1254, 2021.

[7] S. Liu, A. Saoud, P. Jagtap, D. V. Dimarogonas, and M. Zamani, "Compositional synthesis of signal temporal logic tasks via assume-guarantee contracts," in *IEEE 61st Conference on Decision and Control (CDC)*, pp. 2184–2189, IEEE, 2022.

[8] A. Nikou, D. Boskos, J. Tumova, and D. V. Dimarogonas, "Cooperative planning for coupled multi-agent systems under timed temporal specifications," in *2017 American Control Conference (ACC)*, pp. 1847–1852, 2017.

[9] S. Andersson, A. Nikou, and D. V. Dimarogonas, "Control synthesis for multi-agent systems under metric interval temporal logic specifications.," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 2397–2402, 2017. 20th IFAC World Congress.

[10] A. Saoud, P. Jagtap, M. Zamani, and A. Girard, "Compositional abstraction-based synthesis for interconnected systems: An approximate composition approach," *IEEE Transactions on Control of Network Systems*, vol. 8, no. 2, pp. 702–712, 2021.

[11] T. Wongpiromsarn, A. Ulusoy, C. Belta, E. Frazzoli, and D. Rus, "Incremental synthesis of control policies for heterogeneous multi-agent systems with linear temporal logic specifications," in *IEEE International Conference on Robotics and Automation*, pp. 5011–5018, 2013.

[12] R. Alur, S. Moarref, and U. Topcu, "Compositional and symbolic synthesis of reactive controllers for multi-agent systems," *Information and Computation*, vol. 261, pp. 616–633, 2018. 4th International Workshop on Strategic Reasoning.

[13] M. Srinivasan, S. Coogan, and M. Egerstedt, "Control of multi-agent systems with finite time control barrier certificates and temporal logic," in *IEEE Conference on Decision and Control (CDC)*, pp. 1991–1996, 2018.

[14] L. Wang, A. D. Ames, and M. Egerstedt, "Safety barrier certificates for collisions-free multirobot systems," *IEEE Transactions on Robotics*, vol. 33, no. 3, pp. 661–674, 2017.

[15] M. Mizoguchi and T. Ushio, "Abstraction-based symbolic control barrier functions for safety-critical embedded systems," *IEEE Control Systems Letters*, vol. 6, pp. 1436–1441, 2022.

[16] P. Nilsson and A. D. Ames, "Barrier functions: Bridging the gap between planning from specifications and safety-critical control," in *IEEE Conference on Decision and Control (CDC)*, pp. 765–772, 2018.

[17] J. Chen, S. Moarref, and H. Kress-Gazit, "Verifiable control of robotic swarm from high-level specifications," in *Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems*, AAMAS '18, (Richland, SC), p. 568–576, 2018.

[18] A. A. Kurzhanskiy and P. Varaiya, "Reach set computation and control synthesis for discrete-time dynamical systems with disturbances," *Automatica*, vol. 47, no. 7, pp. 1414–1426, 2011.

[19] O. Maler, "Computing reachable sets: An introduction," 2008.

[20] G. Reissig, A. Weber, and M. Rungger, "Feedback refinement relations for the synthesis of symbolic controllers," *IEEE Transactions on Automatic Control*, vol. 62, no. 4, pp. 1781–1796, 2017.

[21] C. Baier and J.-P. Katoen, *Principles of Model Checking*. The MIT Press, 2008.

[22] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, "Control barrier functions: Theory and applications," in *18th European Control Conference (ECC)*, pp. 3420–3431, 2019.

[23] M. Rungger and M. Zamani, "SCOTS: A tool for the synthesis of symbolic controllers," in *Proceedings of the 19th international conference on hybrid systems: Computation and control*, pp. 99–104, 2016.

[24] M. Khaled and M. Zamani, "Omegathreads: Symbolic controller design for ω-regular objectives," in *Proceedings of the 24th International Conference on Hybrid Systems: Computation and Control*, HSCC '21, (New York, NY, USA), Association for Computing Machinery, 2021.

[25] P. Jagtap and M. Zamani, "QUEST: A tool for state-space quantization-free synthesis of symbolic controllers," in *Quantitative Evaluation of Systems* (N. Bertrand and L. Bortolussi, eds.), (Cham), pp. 309–313, Springer International Publishing, 2017.

[26] Y. Xiong, D.-H. Zhai, M. Tavakoli, and Y. Xia, "Discrete-time control barrier function: High-order case and adaptive case," *IEEE Transactions on Cybernetics*, pp. 1–9, 2022.