Trust-based Rate-Tunable Control Barrier Functions for Non-Cooperative Multi-Agent Systems

Hardik Parwana\textsuperscript{1}, Aquib Mustafa\textsuperscript{2}, and Dimitra Panagou\textsuperscript{3}

Abstract—For efficient and robust task accomplishment in multi-agent systems, an agent must be able to distinguish cooperative agents from non-cooperative (i.e., uncooperative and adversarial) agents. In this paper, we first develop a trust metric based on which each agent forms its own belief of how cooperative the other agents are, i.e., of how much the other agents contribute to maintaining safety. With safety encoded as Control Barrier Functions (CBFs), the trust metric is in turn used to adjust the rate at which the CBFs allow the system trajectories to approach the boundary of the safe set. This is achieved via a novel Rate-Tunable CBF, which yields less conservative performance compared to an identity-agnostic implementation, where cooperative and non-cooperative agents are treated similarly. The proposed adaptation and control method is evaluated via simulations on heterogeneous multi-agent systems including non-cooperative agents.

I. INTRODUCTION

Teams of collaborating robots can enable tasks such as payload transportation, surveillance and exploration [1]. The ability to meet specifications such as safety and goal reaching even in the presence of non-cooperative agents is essential to successful operation and mission accomplishment. With safety specifications encoded as Control Barrier Functions (CBFs), this work develops a trust metric with which each agent distinguishes cooperative from non-cooperative agents (the latter include uncooperative and adversarial agents, as defined formally in Section III-2). The trust metric is then used to shape the response of each agent’s controller by adjusting its corresponding CBF parameters. As a motivational example, consider the scenario depicted in Fig.1, where a green robot will be intercepted by a red robot if it follows its nominal trajectory of moving forward. The red robot wishes to cause no harm, but gives priority to its own task of moving along its own nominal trajectory. Hence if the green robot infers, based on previous observations, that the red robot is not chasing the green robot but rather moves along its nominal trajectory, then it (the green robot) can adjust its response and minimize deviation from its nominal trajectory, while maintaining safety with the red robot.

Specifying tasks for multi-agent systems and designing safe controllers for successful execution has been an active research topic [2]–[5]. Control synthesis for multi-agent systems in the presence of non-cooperative agents has also received vivid interest, with many remarkable results [6]–[13]. In [6]–[10], the authors present resilient algorithms for flocking and active target-tracking applications, respectively. In [13] and [12], the authors design game-theoretic and adaptive control mechanisms to directly reject the effect of adversaries without the need of knowing or detecting their identity. Recently, CBF-based approaches have also been presented for achieving resilience under safety and goal-reaching objectives. In particular, [14] developed multi-agent CBFs for non-cooperative agents. [15] designed a mechanism to counter collision-seeking adversaries using CBF-based control that is robust to worst-case actions by the adversaries. All of the above studies either assume that the identities of adversarial agents is known a priori, or they design a robust response without knowing or detecting their identities; nevertheless, as also evidenced by our simulations, both cases can lead to conservative responses. Moreover, most of these works assume further that each agent knows the exact dynamics of the other agents. To the best of our knowledge, no prior studies have employed CBFs to make inferences from the behavior of surrounding agents, and tune their response to reduce conservatism while still ensuring safety.

In this paper, we make two contributions to mitigate the above limitations. First, we define a trust model based on which each agent develops its own belief of how cooperative
the other agents are. Since CBFs ensure safety by restricting the rate of change of barrier functions along the system trajectories [16], we design the trust metric based on how easily these restrictions can be imposed. Each agent rates the behavior of a neighbor agent on a continuous scale, as either 1) being cooperative, i.e., an agent that gives priority to maintaining safety, or 2) being uncooperative, i.e., an agent that does not try to collide, however, gives priority to its own tasks, and thus disregards safety, or 3) being adversarial, i.e., an agent that actively tries to collide with other agents. Second, we design an algorithm that tightens or relaxes a CBF constraint based on this trust metric, and develop Trust-based, Rate-Tunable CBFs (RT-CBFs) that allow online modification of a parameter of the class-\(\mathcal{K}\) function employed with CBFs [16].

Our notion of trust shares inspiration with work that aims to develop beliefs on the behavior of other agents, and then use them for path planning and control. Deep Reinforcement Learning (RL) has been used to learn the underlying interactions in multi-agent scenarios [17], specifically for autonomous car navigation, to output a suitable velocity reference to be followed for maneuvers such as lane changing or merging. A few papers explicitly model trust for a multi-agent system [18]–[20]. In particular, [18] develops an intent filter for soccer-playing robots by comparing the actual movements to predefined intent templates, and gradually updating beliefs over them. Among the studies focusing on human-robot collaboration, [19] learns a Bayesian Network to predict the trust level by training on records of each robot’s performance level and human intervention. [20] defines trust by modeling a driver’s perception of vehicle performance in terms of states such as the relative distance and velocity to other vehicles, and then uses a CBF to maintain the trust above the desired threshold. The aforementioned works show the importance of making inferences from observations. However, they were either developed specifically for semi-autonomous and collaborative human-robot systems using offline data sets, or when they do consider trust, it is mostly computed with a model-free approach, such as RL. The above studies also use the computed trust as a monitoring mechanism rather than being related directly to the low-level controllers that decide the final control input of the agent and ensure safety-critical operation. In this work, we pursue a model-based design of trust metric that actively guides the low-level controller in relaxing or tightening the CBF constraints and helps to ensure successful task completion.

II. Preliminaries

1) Notations: The set of real numbers is denoted as \(\mathbb{R}\) and the non-negative real numbers as \(\mathbb{R}^+\). Given \(x \in \mathbb{R}\), \(y \in \mathbb{R}^n\), and \(z \in \mathbb{R}^{n_i \times m_i}\), \(|x|\) denotes the absolute value of \(x\) and \(||y||\) denotes \(L_2\) norm of \(y\). The interior and boundary of a set \(\mathcal{C}\) are denoted by \(\text{Int}(\mathcal{C})\) and \(\partial\mathcal{C}\). For \(a \in \mathbb{R}^+\), a continuous function \(\alpha : [0, a) \rightarrow [0, \infty)\) is a class-\(\mathcal{K}\) function if it is strictly increasing and \(\alpha(0) = 0\). Furthermore, if \(a = \infty\) and \(\lim_{t \to \infty} \alpha(r) = \infty\), then it is called class-\(\mathcal{K}_\infty\). The angle between any two vectors \(x_1, x_2 \in \mathbb{R}^n, \forall i = 1, 2\) is defined with respect to the inner product as \(\theta = \arccos(||x_1|| ||x_2||)\). Also, \(\delta y\) represents a infinitesimal variation in \(y\).

2) Safety Sets: Consider a nonlinear dynamical system

\[
\dot{x} = f(x) + g(x)u, \tag{1}
\]

where \(x \in \mathcal{X} \subset \mathbb{R}^m\) and \(u \in \mathcal{U} \subset \mathbb{R}^n\) represent the state and control input, and \(f : \mathcal{X} \rightarrow \mathbb{R}^m, g : \mathcal{X} \rightarrow \mathbb{R}^{n_i \times m_i}\) are locally Lipschitz continuous functions. Let a set \(\mathcal{S}\) of safe states be defined as the 0-superlevel set of a continuously differentiable function \(h(x) : \mathcal{X} \rightarrow \mathbb{R}\) as follows:

\[
\mathcal{S} \triangleq \{x \in \mathcal{X} : h(x) \geq 0\}, \tag{2}
\]

\[
\partial \mathcal{S} \triangleq \{x \in \mathcal{X} : h(x) = 0\}, \tag{3}
\]

\[
\text{Int}(\mathcal{S}) \triangleq \{x \in \mathcal{X} : h(x) > 0\}. \tag{4}
\]

Definition 1. (CBF [21]) The function \(h : \mathcal{X} \rightarrow \mathbb{R}\) is a CBF for the system (1) on the set \(\mathcal{S}\) defined in (4) if there exists an extended class-\(\mathcal{K}_\infty\) function \(\nu\) such that

\[
\sup_{u \in \mathcal{U}} \left[ \frac{\partial h}{\partial x} (f(x) + g(x)u) \right] \geq -\nu(h(x)), \forall x \in \mathcal{X}. \tag{5}
\]

Lemma 1. ([21, Theorem 2]) Let \(\mathcal{S} \subset \mathcal{X}\) be the superlevel set of a smooth function \(h : \mathcal{X} \rightarrow \mathbb{R}\). If \(h\) is a CBF on \(\mathcal{S}\), and \(\partial h/\partial x \neq 0 \forall x \in \partial \mathcal{S}\), then any Lipschitz continuous controller for the system (1) belonging to the set

\[
K(x) = \{u \in \mathcal{U} : \frac{\partial h}{\partial x} (f(x) + g(x)u) + \nu(h(x)) \geq 0\}, \tag{6}
\]

renders the set \(\mathcal{S}\) forward invariant (i.e. safe).

In this paper, we assume that \(\nu\) in (17) is given by

\[
\nu(h(x)) = \alpha h(x), \quad \alpha \in \mathbb{R}^+. \tag{7}
\]

With a slight departure from the notion of CBF defined above, \(\alpha\) is treated as a parameter in this work and its value is adjusted depending on the trust that an agent has built on other agents based on their behaviors. Since \(\alpha\) represents the maximum rate at which the state trajectories \(z(t)\) are allowed to approach the boundary \(\partial \mathcal{S}\) of the safe set \(\mathcal{S}\), a higher value of \(\alpha\) corresponds to relaxation of the constraint, which allows agents to get closer to each other, whereas a smaller value tightens it. The design of the trust metric is presented in Section IV.

III. Problem Statement

In this paper, we consider a system consisting of \(N\) agents with \(x_i \in \mathcal{X}_i \subset \mathbb{R}^n_i\) and \(u_i \in \mathcal{U}_i \subset \mathbb{R}^m_i\) representing the state and control input of the agent \(i \in \mathcal{V} = \{1, 2, \ldots, N\}\). The dynamics of each agent is represented as:

\[
\dot{x}_i = f_i(x_i) + g_i(x_i)u_i, \tag{8}
\]

where \(f_i : \mathcal{X} \rightarrow \mathbb{R}^{n_i}, g_i : \mathcal{X} \rightarrow \mathbb{R}^{n_i \times m_i}\) are Lipschitz continuous functions. The dynamics and the control input of an agent \(i\) is not known to any other agent \(j \in \mathcal{V} \setminus i\). However, we make the following assumption on the available observations for each agent.
Assumption 1. Let the combined state of all agents be $x = [x_1^T, ..., x_N^T] ^T \in \mathbb{R}^n$. Each agent $i$ has access to the state vector $x$. Furthermore, the control law for $u_i$, and hence the closed-loop dynamics $\dot{x}_i$, is a locally Lipschitz continuous function of $x$, i.e., $\dot{x}_i = F_i(x)$ where $F_i : \mathbb{R}^n \to \mathbb{R}^{n_i}$ defines the closed-loop dynamics of agent $i$.

The above assumption implies that each agent, including the adversarial and the uncooperative agents, have access to the states of all other agents. However, each agent computes its own control input based on its CBFs that can be different from the CBFs of its neighbors (i.e., $h_{ij} \neq h_{ji}, \alpha_{ij} \neq \alpha_{ji}$ in Section III-1). We also have the following assumption on the estimate that agent $i$ has regarding the closed-loop dynamics $F_j$ of agent $j$.

Assumption 2. Each agent $i$ has knowledge of a set $\tilde{F}_j$ that contains an estimate of the true response $\dot{x}_j$, i.e., such that there exists $b_{F_j} : \mathbb{R}^{n_i} \to \mathbb{R}^+$ for which

$$\dot{x}_j \in \tilde{F}_j = \{ \dot{x}_j \in \mathbb{R}^{n_j} | ||F_j(x) - \dot{x}_j|| \leq b_{F_j}(x) \} . \tag{9}$$

Remark 1. Assumption 2 can easily be realized for systems that exhibit smooth enough motions for a learning algorithm to train on. For example, a Gaussian Process [22] can be used with past observations to infer the motions, within confidence bounds, of the other agents. Another way would be to bound with past observations to infer the motions, within confidence bounds, of the other agents. Therefore, rather than making a fine distinction, this work presents a trust metric that rates other agents on a continuous scale as being cooperative, adversarial or uncooperative. Then, by leveraging the trust metric, an adaptive form of $\alpha_{ij}$ in (10) is presented that adjusts the safety condition for agent $i$ based on the observed behavior of agent $j$.

3) Objective: In this subsection, we first present some definitions and then formulate the objective of this paper.

Definition 3. (Adversarial Agent) An agent $j$ is called adversarial to agent $i$ if agent $j$ chooses its control input $u_j$, and hence its dynamics $\dot{x}_j$, such that

$$\frac{\partial h_{ij}}{\partial x_j} \dot{x}_j \leq 0 \ \forall x_i \in \mathbb{R}^{n_i}, \ x_j \in \mathbb{R}^{n_j}. \tag{11}$$

Definition 4. (Uncooperative Agent) An agent $j$ is called uncooperative to agent $i$ if the control law for $u_j$ is not a function of the state $x_i$ of agent $i$.

Note that the behaviors resulting from these three types of agents when more than two agents are present are not mutually exclusive, and that a cooperative agent might be forced to behave as an adversarial agent under the influence of other agents. Hence, while all the agents are assumed to behave in one of the above ways, the complex nature of interactions in a multi-agent system makes it hard to distinguish them. Moreover, it is not necessary that $h_{ij} = h_{ji}$ and $\alpha_{ij} = \alpha_{ji}$; for example, agents $i$ and $j$ may have different safety radii for collision avoidance. In addition, an agent $i$ may perceive a cooperative agent $j$ to be uncooperative if $j$ cannot satisfy $i$’s prescribed level of safety, given by $\alpha_{ij}$, under the influence of a truly uncooperative or adversarial agent $k$. Therefore, $\alpha_{ij}$ as defined in (10) is presented that adjusts the safety condition for agent $i$ based on the observed behavior of agent $j$.

3) Objective: In this subsection, we first present some definitions and then formulate the objective of this paper.

Definition 5. (Nominal Direction) A nominal motion direction $\dot{x}_i^n$ for agent $i$ is defined with respect to its global task and its Lyapunov function $V_i$ as follows:

$$\dot{x}_i^n = -\gamma \frac{\partial V_i}{\partial x_i} \tag{12}$$

Definition 6. (Nominal Trajectory) A trajectory $x_i^n(t)$ is called the nominal trajectory for an agent $i$, if the agent follows the dynamics in (8) with some $x_i(0) \in \mathcal{X}$ and under control action $u_i = -\gamma \frac{\partial V_i}{\partial x_i}/||\frac{\partial V_i}{\partial x_i}||$, where $\gamma \in \mathbb{R}^+$ denotes some design gain.

We now define the objective of this paper. The problem is as follows.

Objective 1. Consider a multi-agent system of $N$ agents governed by the dynamics given by (1), with the set of agents denoted as $\mathcal{V}$, $|\mathcal{V}| = N$, the set of intact agents denoted as $\mathcal{N}$, the set of adversarial and uncooperative agents denoted as $\mathcal{A} \neq \emptyset$, with $\mathcal{V} = \mathcal{N} \cup \mathcal{A}$. Assume that the identities of the adversarial and the uncooperative agents are unknown. Each agent $i$ has a global task encoded via a Lyapunov function $V_i$, and $N$ local tasks encoded as barrier functions $h_{ij}, j \in \mathcal{V}$. Design a decentralized controller to be implemented by each intact agent $i \in \mathcal{N}$ such that

1) $h_{ij}(t) \geq 0, \ \forall t \geq 0, \ \text{for all} \ i \in \mathcal{N}, j \in \mathcal{V}.$
2) The deviation between the actual trajectory \( x_i(t) \) and the nominal trajectory \( x_i^0(t) \) for agent \( i \) is minimized, where the nominal trajectory is defined in Def. 6.

IV. METHODOLOGY

In this section, we start by introducing a standard form of a QP-based controller that can be used to enforce multiple barrier constraints simultaneously. Next, we propose our new formulation of Rate-Tunable CBFs that allow us to dynamically change class-K function to make the CBF derivative condition more or less strict. Finally, we introduce a trust metric that helps design the dynamics of the class-K function and enables adaptation in multi-agent systems.

The intact agents compute their control input in two steps. The first step computes a reference control input \( u_i^r \) for an agent \( i \) that forces it to track its nominal trajectory \( x_i^0(t) \). The reference control input \( u_i^r \) is designed using the exponentially stabilizing CLF conditions as follows:

\[
\begin{align*}
    u_i^r(x) &= \arg \min_{u \in U_i} \ u^T u \\ 
    \text{s.t.} \quad \dot{V}(x_i, u_i) &\leq -kV(x_i, x_i^0), \quad (13a)
\end{align*}
\]

where \( V_i = ||x_i - x_i^0||^2 \) and \( k > 0 \). In the second step, the following CBF-QP is defined to minimally modify \( u_i^r \) while satisfying (10) for all agents \( j \in V \setminus i \):

\[
\begin{align*}
    u_i(x, \alpha_{ij}) &= \arg \min_{u} \ ||u - u_i^r||^2 \\ 
    \text{s.t.} \quad \frac{\partial h_{ij}}{\partial x_i} \dot{x}_i + \min_{\hat{x}_j \in F_j} \left\{ \frac{\partial h_{ij}}{\partial x_j} \hat{x}_j \right\} &
    \geq -\alpha_{ij} h_{ij}, \forall j \in V \setminus i. \quad (14a)
\end{align*}
\]

where \( \alpha_{ij} \in \mathbb{R}^+ \), and \( \hat{h}_j \) denotes all possible movements of agent \( j \) per Assumption 2. Eq. (14b) provides safety assurance for \( i \) w.r.t the worst-case predicted motion of \( j \). Henceforth, whenever we refer to the actual motion of any agent \( j \) with respect to \( i \), we will be referring to the estimate in the set \( F_j(x) \) that minimizes the contribution to safety, i.e.,

\[
\hat{a}_j^* = \arg \min_{\hat{x}_j \in F_j} \left\{ \frac{\partial h_{ij}}{\partial x_j} \hat{x}_j \right\}. \quad (15)
\]

In the following sections, we first propose the Tunable-CBF as a method that allows us to relax or tighten the CBF constraints while still ensuring safety. Then, we design the trust metric to adjust \( \alpha_{ij} \) and tune the controller response.

A. Rate-Tunable Control Barrier Functions

In contrast to the standard CBF where the parameter \( \alpha \) in (10) is fixed, we aim to design a method to adapt the values of \( \alpha \) depending on the trust metric that will be designed in Section IV-B. In this section, we show that treating \( \alpha \) as a state with Lipschitz continuous dynamics can still ensure forward invariance of the safe set.

Definition 7. (Rate-Tunable CBF) Consider the system dynamics in (1), augmented with the state \( \alpha \in \mathbb{R}^+ \) that obeys the dynamics

\[
\begin{bmatrix}
\dot{x} \\
\dot{\alpha}
\end{bmatrix} = \begin{bmatrix}
f(x) + g(x)u \\
f'(x, \alpha)
\end{bmatrix},
\]

where \( f' : \mathcal{X} \times \mathbb{R} \rightarrow \mathbb{R} \) is a locally Lipschitz continuous function w.r.t \( x, \alpha \). Let \( S \) be the safe set defined as in (4). The function \( h : \mathcal{X} \rightarrow \mathbb{R} \) is a Rate Tunable-CBF for the augmented system (16) on the set \( S \) if there exists a compact set \( A \subset \mathbb{R}^+ \) such that

\[
\sup_{u \in \mathcal{U}} \left[ \frac{\partial h(x)}{\partial x} (f(x) + g(x)u) \right] \geq -\alpha h(x) \quad \forall x \in \mathcal{X}, \alpha \in A
\]

(17)

Theorem 1. Consider the augmented system (16), and a safe set \( S \) in (4) be defined by a Rate-Tunable CBF \( h \). For a locally Lipschitz continuous reference controller \( u^r : \mathcal{X} \rightarrow \mathcal{R}^m \), let the controller \( u = \pi(x, \alpha) \), where \( \pi : \mathcal{X} \times \mathcal{R}^+ \rightarrow \mathcal{U} \) be formulated as

\[
\pi(x, \alpha) = \arg \min_{w \in \mathcal{U}} ||u - u^r||^2 \quad (18a)
\]

s.t. \( \frac{\partial h}{\partial x} (f(x) + g(x)u) \geq -\alpha h(x) \) (18b)

where \( \frac{\partial h}{\partial x} \) is also locally Lipschitz continuous. Suppose there exists \( \hat{h} > 0 \) such that \( h(x) < \hat{h} \forall x \in S \). Then, the set \( S \) is forward invariant.

Proof. Step 1: Since \( h \) is a Rate-Tunable CBF, according to (17), there always exists a \( u \in \mathcal{R}^m \) that satisfies the constraint of the QP (18b). The solution \( \pi(x, \alpha) \) is also unique as the optimization problem is strictly convex. Since \( f, g, h, \frac{\partial h}{\partial x}, \frac{\partial h}{\partial x} \) are locally Lipschitz, by composition, \( \frac{\partial h}{\partial x} f(x), \frac{\partial h}{\partial x} g(x) \) are also locally Lipschitz. By [16, Thm. 3], it follows that \( \pi \) is locally Lipschitz continuous.

Step 2: Since \( \pi \), and hence the closed-loop dynamics, is locally Lipschitz continuous, (16) admits a unique solution over its interval of existence. Let us consider the evolution of \( h \) trajectory for this system now. Since the set \( A \) is compact, \( \exists \gamma \in \mathbb{R}^+ \) such that \( -\alpha h \geq -\gamma h, \forall \alpha \in A \). Consider the system governed by \( \dot{h} = -\gamma h \). From [23, Lemma 4.4], this systems admits a unique solution for all \( t < 0 \) and is lower bounded by 0. Therefore, using comparison lemma [23, Lemma 3.4], the systems governed by \( \dot{h} \geq -\gamma h \) and \( h \geq -\alpha h \), over their respective interval of existence, are also lower bounded by 0. Since \( h \) is also upper bounded, it evolves on a compact set \( S_h = \{h \mid 0 \leq h \leq \hat{h} \} \). Therefore, from [23, Thm 3.2] the system \( \dot{h} \geq -\alpha h \) admits a solution globally, i.e., for \( \forall t > 0 \). Hence the set \( S \) is forward invariant.

B. Design of Trust Metric

The margin by which the CBF condition (10) is satisfied, i.e., the value of \( h_{ij} + \alpha_{ij} h_{ij} \), as well as the best action that agent \( i \) can implement to increase this margin for a given motion \( \dot{x}_j \) of agent \( j \), are both important cues that help infer the nature of agent \( j \). The adaptation of the parameters \( \alpha_{ij} \) by agent \( i \) depends on the following:

1) Allowed motions of agent \( j \): The worst that an agent \( j \) is allowed to perform in agent \( i \)'s perspective is the critical point beyond which agent \( i \) cannot find a feasible solution
perplane has the normal direction 

Equation (20) represents a halfspace whose separating hy-

which possible motion is more trustworthy. If 

This gives an additional degree of freedom for deciding 

This gives a lower bound that, if violated by agent 

The two quantities of interest from Fig. 2 are the distance 

1) Distance-based Trust Score: Let the half-space in (20) 

where \( d^n_j \) is an incompatible vector, corresponding to 

2) Direction-based Trust Score: Suppose the angle 

3) Final Trust Score: The direction-based trust 

where \( f_\theta : \mathbb{R}^+ \rightarrow [0,1] \) is a monotonically-increasing, 

Lipschitz continuous function, such that \( f_\theta(0) = 0 \). A 

A possible choice would be \( f_\theta(d) = \tanh(\beta d) \), with \( \beta \) being 

a scaling parameter. 

Note that even if \( \theta^n_j = \theta^n_a \), i.e., \( j \) is perfectly following its nominal 

direction, we do not design \( f_\theta \) to be 1 as the robot might be 

uncooperative. We give \( f_\theta \) higher values when \( \theta^n_j < \theta^n_a \), as with \( a_{j2} \) in Fig. 2, \( j \) seems to be compromising its nominal 

movement direction for improved safety, thus leading to a 

higher score. Finally, when \( \theta^n_j < \theta^n_a \), as with \( a_{j3} \) in Fig. 2, then \( j \)'s current motion is performing worse for inter-

robot safety than its nominal motion and is therefore either 

uncooperative/adversarial or under the influence of other 

robots, both of which lead to lower trust. 

3) Final Trust Score: The trust metric is now designed 

based on \( \rho_d \) and \( \rho_\theta \). Let \( \bar{\rho}_d \in (0,1) \) be the desired minimum 

robustness in satisfying the CBF condition. Then, the trust 

metric \( \rho \in [-1,1] \) is designed as follows: 

\[
\rho = \begin{cases} 
(\rho_d - \bar{\rho}_d)\rho_\theta, & \text{if } \rho_d \geq \bar{\rho}_d, \\
(\rho_d - \bar{\rho}_d)(1 - \rho_\theta), & \text{if } \rho_d < \bar{\rho}_d. 
\end{cases}
\] (26) 

Here, \( \rho = 1, -1 \) represent the absolute belief in another agent 

being cooperative and adversary, respectively. If \( \rho_d > \bar{\rho}_d, \)


\[
\rho_d = f_d(d^n_j),
\] (24) 

Equation (20) represents a halfspace whose separating hy-

perplane has the normal direction \( \hat{s} = \frac{\partial h_{ij}}{\partial x_j} \), and has been 

visualized in Fig. 2. 

(2) Actual motion of agent \( j \): This is given by Eq. (15). 

(3) Nominal behavior of agent \( j \): Suppose that agent \( i \) has 

knowledge of agent \( j \)'s target state. A nominal direction of 
motion \( \hat{n}_j \) of agent \( j \) in agent \( i \)'s perspective can be obtained 

using the Lyapunov function \( V^j_i = ||x_j - x^n_j||^2 \) as: 

\[
\hat{n}_j = -\frac{\frac{\partial V^j_i}{\partial x_j}}{||\frac{\partial V^j_i}{\partial x_j}||}.
\] (22) 

Knowledge of nominal direction plays an important role in 

shaping belief as it helps to distinguish between uncoopera-
tive and adversarial agents. Note that infinitely many values 

of \( \hat{x}_j \) may satisfy the CBF derivative condition in the same 

way (i.e., will have the same \( d^n_j \) in Fig. 2 as explained later). 

This gives an additional degree of freedom for deciding 

which possible motion is more trustworthy. If \( \hat{x}_j \) is behaving 

worse than the nominal direction, then it is a cause of concern 
as it is not consistent with the belief of agent \( i \) for agent \( j \). 

Note that \( x^n_j \) need not be the true target state of agent \( j \) 

for our algorithm to work since if \( x^n_j \) is not known, we can 

consider the worst-case scenario where \( x^n_j = x_i \), i.e., that \( j \) 
is an adversary and targets to collide with agent \( i \); over time, 

our algorithm will learn that \( j \) is not moving along \( \hat{x}^j \), and 

therefore increases \( i \)'s trust of \( j \). 

Fig. 2: Illustration of the halfspaces induced by the constraint function. \( Av \geq b \) represents the halfspace described by (20) with 
\( A = \frac{\partial h_{ij}}{\partial x_j}, v = \hat{x}_j, \) and \( b = -\alpha h - \max \{ \frac{\partial h_{ij}}{\partial x_i} \} \). \( a_{j1}, a_{j2} \) are two instances of the actual motion of agent \( j \). \( \hat{s} \) is the normal to the 
hyperplane \( Av = b \). \( n_j \) is the nominal direction of motion for 
agent \( j \).
then we would like to have $\rho > 0$, and its magnitude is scaled by $\rho_d$ with smaller values of $\rho_d$ conveying low trust. Whereas, if $\rho_d < \rho_d$, then we would like the trust factor to be negative. A smaller $\rho_d$ in this case implies more distrust and should make the magnitude larger, hence the term $1 - \rho_d$.

The trust $\rho$ is now used to adapt $\alpha$ with following equation

$$\dot{\alpha}_{ij} = f_{\alpha_{ij}}(\rho),$$

where $f_{\alpha_{ij}} : [-1, 1] \rightarrow \mathbb{R}$ is a monotonically increasing function. A positive value of $f_{\alpha_{ij}}$ relaxes the CBF condition by increasing $\alpha$, and a negative value decreases $\alpha$. The framework that each agent $i$ implements at every time $t$ is detailed in Algorithm 1.

Algorithm 1 Trust-based Multi-agent CBF

Require: $x, i, f_\alpha, f_\theta, f', \rho_d$
1: $\alpha_{ij} \leftarrow$ Current value of CBF Parameters
2: for all time do
3: for $j \in \mathcal{V} \setminus i$ do
4: Predict $\alpha_j$ > Actual movement of $j$
5: Compute $\rho_\theta, \rho_d$ with Eqns.(25),(24)
6: Compute $\rho$ with (26) > Trust score
7: Calculate nominal input using (13).
8: Implement $u_j$ from (14).
9: Update $\alpha_{ij}$ with update rule (27)
10: end for
11: end for

Remark 2. Note that equation (26) does not represent a locally Lipschitz continuous function of $\rho_\theta, \rho_d$. This poses theoretical issues as having a non-Lipschitz gradient flow in (27) would warrant further analysis concerning existence of unique solution for the combined dynamical involving $x$ and $\alpha$. Hence, while (26) represents our desired characteristics, we can use a sigmoid function to switch across the boundary $\rho_d = \rho_d$ thereby holding the assumptions in Theorem 1 true.

C. Sufficient Conditions for a Valid trust Metric

In the presence of multiple constraints, feasibility of the QP (14) might not be guaranteed even if the control input is unbounded and the states are far away from boundary, i.e., $h_{ij} >> 0$. In this section, we derive conditions that guarantee that the QP does not become infeasible.

Assumption 3. Suppose the initial state satisfies the barrier constraints strictly, i.e., $h_{ij}(x_i(0), x_j(0)) > 0$, $j \in \mathcal{V} \setminus i$. Now suppose at each time $t$, there always exist $\alpha_{ij} > 0$ such that the QP (14) is feasible, then $h_{ij}(x_i(t), x_j(t)) > 0 \forall t > 0$.

Theorem 2. (Compatibility of Multiple CBF Constraints)
Under Assumptions 1-3, consider the system dynamics in (1) subject to multiple barrier functions $h_j, j \in \mathcal{V}_M = 1, 2, ..., M$. Let the controller $u(x, \alpha)$, with $\alpha = \{\alpha_j | j \in \mathcal{V}_M\}$, be formulated as

$$u(x, \alpha) = \arg\min_u \|u - u^r\|^2$$

s.t. $h_j(x, u) \geq -\alpha_j h_j(x), \forall j \in \mathcal{V}_M$, (28b)

with corresponding parameters $\alpha_j$. Now suppose $\alpha_j$, as an augmented state, has following dynamics

$$\dot{\alpha}_j = f_j(x, \alpha_1, \alpha_2, ..., \alpha_M).$$

Suppose the solution of QP in (28), the control $u(x, \alpha) \in \mathcal{U}$, is always locally Lipschitz continuous in $x$ and $\alpha$ so that the closed-loop dynamics of $x$ be denoted as $\dot{x} = F(x)$ is locally Lipschitz continuous. Let $L_{h_j}, L_{\theta_j}$, and $L_F$ be the Lipschitz constants of $h_j(x), \dot{h}_j(x, \dot{x})$ and $F(x)$. In case of imperfect information, we assume an estimate $\hat{F}(x)$ is available such that $\|F(x) - \hat{F}(x)\| \leq b_F(x)$. Further, assume that solution of Suppose a solution to (28) exists at initial time $t = 0$ and $\dot{\alpha}_j$ satisfies the following condition with $B(x) = \|\hat{F}(x)\| + b_F(x)$ (see Assumption 2)

$$\dot{\alpha}_j \geq - \left( d_j + L_{h_j} B(x)(L_F + 1) + \alpha_j L_{h_j} B(x) \right) \frac{1}{L_{h_j}}.$$

Then, a solution to (28) continues to exist until $h_j = 0$ for any $j \in \mathcal{V}_M$.

Proof. Based on Lipschitz property, we have $\delta \dot{x} \leq L_F \|\delta x\|$, where $\delta y$ denotes infinitesimal variation in $y$. In order to have a feasible solution for QP in (28), it should hold that

$$d_j(x, \dot{x}) = \dot{h}_j(x, \dot{x}) + \alpha_j h_j(x) \geq 0.$$ (31)

The variation in $d_j(x, \dot{x})$ is given by

$$\delta d_j = \delta \dot{h}_j + h_j \delta \alpha_j + \alpha_j \delta h_j.$$ (32)

For a feasible solution to QP in (28) with variation in $\delta d_j$, one needs $d_j + \delta d_j \geq 0$. Thus, the following condition holds

$$\delta \alpha_j \geq - \left( d_j + \delta \dot{h}_j + \alpha_j \delta h_j \right) \frac{1}{L_{h_j}}.$$ (33)

In the multi-agent setting, since each constraint expresses pairwise safety among two robots $j_1, j_2 \in \{1, 2, ..., N\}$, it follows that $h_j$ depends only on a subset of the state vector $x$, namely on $x_{j_1}, x_{j_2}$. However, the evolution of state dynamics $\dot{x}$ depends on the control input $u$ computed based on the QP formulation in (28), where $u$ depends on all constraints $h_j$ and states $x_j$. Thus, $\delta \dot{h}_j$ and $\delta \dot{x}$ are dependent on the states of all agents and not only on $x_{j_1}, x_{j_2}$. This introduces coupling between the constraints, which is hard to solve for analytically. However, given that we assume that $\dot{x} = F(x)$ with a known Lipschitz constant $L_F$, we can decouple all constraints. Using $\|\delta \dot{x}\| \leq L_F \|\delta x\|$, $\|\delta h_j(x)\| \leq L_{h_j} \|\delta x\|$, and $\|\delta \dot{h}_j(x, \dot{x})\| \leq L_{h_j} (\|\delta x\| + \|\delta \dot{x}\|)$, we can write (33) as
\[ \delta x_j \geq -\left(d_j + L_h \|\delta x\| + \|\delta x_j\| + \alpha_j L_h \|\delta x\|\right) \frac{1}{h_j}. \]

Finally, since we are interested in infinitesimal variations with time, the change \( \delta x \) is specifically given by the dynamics as \( \delta x = F(x) \). From Assumption 2, we further have a bound available on \( \|F(x)\| \) which is \( B(x) = \|F(x)\| + b_F(x) \). Therefore, if \( \dot{\alpha} \) satisfies (30), we have that \( \dot{d}_j + \dot{d}_j \geq 0, \forall j \) and hence a solution for QP in (28) exists. This completes the proof.

**Remark 3.** Consider a boundary condition scenario, i.e., when \( h_j \to 0 \) for which \( \alpha_j \to \infty \). Such scenario can happen, for example, when an agent is surrounded by adversaries and has no escape path. In order to keep the QP feasible, the agent will have to keep increasing \( \alpha_j \) until \( h_j = 0 \) and then collision is unavoidable. We would expect that if there were an escape direction, then at least one of \( \alpha_j \) would have lower bound \( \leq 0 \) before \( h_j = 0 \) is reached. Note that in case of \( \alpha_j \to \infty \) in finite time, the assumption on local Lipschitzness of \( u \) and \( h_j \) might no longer hold. Such an analysis will be formally addressed in future work.

V. Simulation Results

The proposed Algorithm 1 is implemented to design controllers for waypoint navigation of a group of three intact robots while satisfying desired constraints. The intact agents are modeled as unicycles with states given by the position coordinates \( p_x, p_y \) and the heading angle \( \psi \) w.r.t. a global reference frame, \( \dot{p}_x = v \cos \theta, \dot{p}_y = v \sin \theta, \psi = \omega \), where \( v, \omega \) are linear and angular velocity expressed in the body-fixed frame, and act as control inputs. The adversarial and uncooperative agents are modeled as single integrators with dynamics \( \dot{p}_x = v_x, \dot{p}_y = v_y \), where \( v_x, v_y \) are velocity control inputs. Fig. 3 shows a scenario where an adversarial robot chases one of the intact agents, and two other uncooperative agents move along horizontal paths without regard to any other agent. The nominal trajectories in this case are straight lines from initial to target locations. None of the intact robots know the identity of any other robot in the system, and initialize \( \alpha_{ij} \) to 0.8 uniformly. It can be seen that intact agents are successfully able to remain close to the nominal paths and reach their target location in given time. For comparison, we also show trajectories for fixed \( \alpha \) (non-adaptive) case. For \( \alpha = 0.8 \), no solution exists to the QP (14) after some time, and the simulation fails. Therefore, we simulate another scenario where we assume to know identities of agents beforehand. \( \alpha \) for adversaries is chosen to be 2.0 for intact (cooperative) agents, and for 0.8 for others. Even with these choices for \( \alpha \), the intact agents fail to reach the goal and diverge away from their nominal paths. Note that our method saves us the effort to identify agents and then choose proper \( \alpha \) for them. Fig. 4, 5, and 6 illustrate the variation of trust metric, \( \alpha_{ij} \) s, and CBFs with time. The adversarial agent uses an exponentially stabilizing CLF to chase agent 1. The reference velocity for unicycles using was computed with a controller of the form: \( v = k_x e_x, \omega = k_\omega (\arctan(e_y/e_x) - \psi) \), where \( k_x, k_\omega > 0 \) are gains, both taken as 2.0 in simulations, \( e_x, e_y \) are position errors of the agent to its nominal trajectory in \( X,Y \) coordinates respectively. The trust metric was computed using (26) with \( \rho_d = 1.0 \). We use first-order barrier functions for the unicycle model [24] to enforce collision avoidance, and \( f_d = \tanh(d), f_\theta = \tanh(2\theta^1/\theta^2) \) in Eqns. (24),(25). The simulation video and code can be found at https://github.com/hardikparwana/Adversary-CBF

Assumption 2 was realized by assuming (and verifying through observations) that the maximum normed difference between \( \dot{x}_i(t) \), which is to be predicted, and \( \dot{x}_i(t-\Delta t) \), is 10% of the norm of \( \dot{x}_i(t-\Delta t) \). This is reasonable as the simulation time step \( \Delta t \) is 0.05 sec, and because the adversaries and intact agents all use Lipschitz continuous controllers. Note that the case with fixed \( \alpha \) in Fig. 3 uses the same assumption to design a controller, but still fails to reach the goal.

A. Conclusion and Future Work

This paper introduces the notion of trust for multi-agent systems where the identity of robots is unknown. The trust metric is based on the ease of satisfaction of CBF constraints. It also provides a direct feedback to the low-level controller and help shape a less conservative response while ensuring safety. The effect of input constraints and the sensitivity of the algorithm to its parameters and function choices will be evaluated in future work.

REFERENCES

Fig. 4: Trust between different pairs of robots. Note that two agents need not have the same level of trust for each other. The initial trust for adversary is positive. This is because the initial value of $\alpha = 0.8$ is already a very conservative value and trust based relation allows agent 1 to not deviate too much from nominal trajectory but still avoids collision.

Fig. 5: Variation of the parameters $\alpha_{1j}$ of Robot 1 with respect to Robot $j=2,3$ and the adversarial agent. Trust-based adaptation allows robot 1’s $\alpha$ to increase, thus relaxing the constraints.


Fig. 6: Variation of barrier functions of Robot 1 with time. The plots represent the value of barrier function used by agent 1 for collision avoidance with agent 2,3 and the adversarial agent. The barriers with uncooperative agents are not shown but can be found along with our videos. Trust-based relaxation allows agents to go closer to the safe set boundary ($h_{ij} = 0$) compared to fixed $\alpha$ case, and hence leads to less conservative response while still guaranteeing safety.


