Unmanned Systems

https://www.worldscientific.com/worldscinet/us

Realization of Robust Formation for Multi-UAV Systems Using Control Barrier Functions

Zhaoming Zhang ⓘ*, Yiming Wu ⓘ*,‡, Jie Jiang ⓘ*, Ning Zheng ⓘ*, Wei Meng ⓘ†

*School of Cyberspace, Hangzhou Dianzi University,
Hangzhou 310018, P. R. China

†School of Automation, Guangdong University of Technology,
Guangzhou 510006, P. R. China

Network robustness is a necessary prerequisite for the effective execution of resilient control in distributed multiple unmanned aerial vehicles (UAVs). However, it remains a challenging task to construct a communication graph that satisfies specific network robustness properties. This paper investigates robust formation control of multi-UAV systems using control barrier functions (CBFs). We first propose a novel formation law to drive groups of UAVs into formations with communication graphs that satisfy the (r, s)-robustness. With such a law, all the normal UAVs in the formation are capable of executing a given resilient consensus protocol, and achieving convergence in the presence of malicious attackers. Then, we present a control law that facilitates the establishment of UAV formations, in which the communication graphs satisfy p-fraction robustness. Finally, simulation examples are given to verify the effectiveness of the proposed formation control laws.

Keywords: Distributed systems; robust formation; multi-UAV; control barrier function.

1. Introduction

In recent years, the cooperative control of multiple unmanned aerial vehicles (UAVs) has gained much attention, due to its wide applications ranging from civil [1–3] to military missions [4–6]. Some key issues of multi-UAV systems have been extensively studied by scholars, such as containment control [7, 8], path planning [9, 10] and collision avoidance [11, 12]. Zhi *et al.* [7] investigated the cooperative control of formation flight for fixed-wing UAVs. In [8], the authors proposed a control strategy for guiding robots in multi-robot systems toward a target region, even in the presence of adversarial interference. Path following is the process to track a specified path with high accuracy, [10] has settled the cooperative moving path following problem with speed constraints. Yao *et al.* in [13] proposed

a problem called Vector Field-based integrated Collision Avoidance and Path Following problem (VF-CAPF) and solved it by designing a switching composite vector field, ensuring multi-UAV system effective path-following. Recent work in [11] proposed a novel method for ensuring the stability and safety of nonlinear multi-UAV systems by integrating the design of control Lyapunov functions (CLFs) and control barrier functions (CBFs).

Formation control plays a crucial role in addressing the multi-UAV cooperative control problems [14]. It is essential to develop either a centralized or distributed controller to ensure the successful completion of the formation task by all UAVs. Up to now, many formation strategies have appeared, such as leader–follower [15, 16], virtual structure [17], and artificial potential field [18]. Wei *et al.* [15] presented an adaptive leader-following formation tracking control methodology that addresses disturbances, safety concerns, and sensing limitations in spacecraft formation tracking. Recent work [16] explored leader-following synchronization in coupled harmonic oscillators, offering efficient protocols and quantifying synchronization errors.

Paper [17] studied formation problems based on virtual structure, the virtual structure has a broad application and can guarantee the formation when a UAV has damaged. Li *et al.* [18] proposed an extended virtual force approach to improve self-deployment in mobile sensor networks.

In addition, many advanced control methods have emerged to enhance the performance of multi-UAV formations, such as adaptive control [19, 20], finite-time control [21, 22], optimal formation [23, 24], and learning-based formation [25, 26]. Ames *et al.* [19] employed quadratic programming to amalgamate CLFs and CBFs, facilitating the implementation of an adaptive control scheme for the multi-agent system. Li *et al.* [21] proposed Finite-time Convergence Control Barrier Function (FCBF) to ensure proper behavior sequencing within a finite time in multi-robot systems. In [23], a feedback linearization method was used to convert the nonlinear model into a linear model, and an optimal controller was designed to realize the multi-UAV formation. Some intelligence methods have also been proposed for the formation control of multi-agent systems [25–27].

However, most existing research on the formation problem is mainly based on an ideal network environment, and rarely consider the impact of network attacks on multi-UAV formation. Recently, the problem of robust formation, that is, designing suitable control protocols to drive UAVs in finite time into formations with robust communication graphs, has received increasing attention [23, 28]. Among the existing measures of communication network robustness, the work in [29] exploits an important graph property called *r*-robustness, which provides sufficient conditions for distributed resilient algorithms to the networked control systems. The *r*-robustness quantifies the network graph topology conditions under which normal nodes in the system can still complete the consensus algorithm in the presence of malicious nodes. For instance, in scenarios where nodes within the system encounter a maximum of F malicious nodes, if the network communication topology adheres to a $(2F+1)$-robust graph and the normal nodes execute the Weight-Mean-Subsequence-Reduced (W-MSR) distributed consensus algorithm, it is demonstrated that, under these conditions, all normal nodes ultimately achieve the resilient consensus [30]. In particular, Guerrero-Bonilla and Kumar [23] propose a formation method based on CBF control law, which enables the network completed by the formation to have *r*-robustness, thereby enabling multi-UAV systems to achieve consensus algorithms under malicious attacks.

Based on the above observations, this paper is concerned with the robust formation problem for UAVs, whose goal is to achieve consensus in the presence of malicious attacks. Building upon the previous work in [23], we introduce two novel formation strategies that systematically construct (r,s)-robust and *p-fraction* robust multi-UAV networks, commencing with an arbitrary assortment of UAVs. The methods proposed in this paper further enhance the ability of the constructed multi-UAV formations to resist potential network attacks. The main contributions of the paper are as follows:

(1) This study first introduces the concept of osmosis nodes, defining them as nodes with significant critical influence within a distributed system. Through a thorough analysis of the presence of osmosis nodes at various proportions in the system, we unveil the diversity of characteristics they impart to the network topology properties.
(2) Furthermore, we conducted an in-depth investigation into the number of connected vertices and their associated connection attributes within the graph, with a particular emphasis on the interrelationships under the condition of satisfying the *p-fraction* robust property.
(3) We consider these graph-theoretic findings as the primary contributions of this paper, comprising a set of control laws designed to guide UAVs into formations that satisfy both (r,s)-robustness and *p-fraction* robustness, while specifying only the required number of neighbors for communication.

The structure of the remaining sections in this paper is as follows. Section 2 provides an overview of the essential knowledge required to understand the research problem. Section 3 introduces the theorems associated with constructing both (r,s)-robust and *p-fraction* formations. In Sec. 4, the CBF is developed based on the theorems presented in Sec. 3. Section 5 validates the theoretical feasibility of the paper through simulation analysis. Lastly, Sec. 6 provides a summary of the research findings.

Notations: In the context of our investigation, the symbols $\mathbb{N}$, $\mathbb{R}$, and $\mathbb{R}^+$ signify the sets of natural numbers, real numbers, and positive real numbers, respectively. Simultaneously considering $\mathcal{A}$ and $\mathcal{B}$ as two distinct sets, $|\mathcal{A}|$ denotes the cardinality of set $\mathcal{A}$, and we use $\mathcal{A} \cup \mathcal{B}$, $\mathcal{A} \cap \mathcal{B}$, and $\mathcal{A} \backslash \mathcal{B}$ to express the union, intersection, and set difference, respectively.

2.   Preliminaries and Problem Formulation

2.1.   *Graph theory and network robustness*

A directed graph is described by a pair $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is a set of nodes and $\mathcal{E}$ is a set of edges, in which an edge $(i,j) \in \mathcal{E}$ connects nodes i and j from $\mathcal{V}$. The set of neighbors of node i is denoted by $\mathcal{V}_i = \{j \in \mathcal{V} | (i,j) \in \mathcal{E}\}$, and the degree of a node i is denoted by $|\mathcal{V}_i|$. To achieve consensus, node i shares a value η_i with its network neighbors, and

updates its value over time following a nominal rule given by

$$\eta_i[t+1] = w_{ii}[t]\eta_i[t] + \sum_{j \in \mathcal{V}_i[t]} w_{ij}[t]\eta_{ji}[t], \tag{1}$$

where $\eta_{ji}[t]$ represents the shared value from neighbor j to i at time t, $w_{ij}[t] = 0$ whenever $j \notin \mathcal{V}_i[t]$, $w_{ij}[t] > \alpha$ for some $\alpha \in (0,1)$, and $\sum_j w_{ij}[t] = 1$, for all $i \in \mathcal{V}$ and $t \in \mathbb{Z}_{\geq 0}$. Consensus is achieved under these conditions when the graph exhibits a rooted out-branching [31, 32].

Definition 2.1 (Malicious Attacker). A node $i \in \mathcal{V}$ is deemed malicious if it persistently sends $\eta_i[t]$ to all its neighbors at each discrete time-step, but deviates from the standard update rule (1) at arbitrary time-steps.

The W-MSR algorithm, proposed in [29], ensures consensus in distributed networked systems even in the presence of malicious attackers. The basic operation of W-MSR algorithm involves each node discarding values that are either strictly smaller or strictly larger than its own value by a factor of F or f_{attacker}. Subsequently, the nominal rule is applied using the remaining values. For further details, see [29, 30].

The graph property, referred to as robustness and defined below, establishes necessary conditions for the W-MSR algorithm to guarantee consensus.

Definition 2.2 (F-Local Set, [29]). A set $\mathcal{S} \subset \mathcal{V}$ is termed F-local if at any given time-step t, it includes no more than F nodes from the neighborhoods of all nodes outside of $\mathcal{S}$. Formally, this condition is represented as $|\mathcal{V}_i[t] \bigcap \mathcal{S}| \leq F$, $\forall i \in \mathcal{V} \backslash S, \forall t \in \mathbb{Z} \geq 0, F \in \mathbb{Z}_{\geq 0}$.

Definition 2.3 (f_{attacker}-fraction Local Set, [30]). A set $\mathcal{S} \subset \mathcal{V}$ is f_{attacker}-*fraction* local if it contains at most a fraction f_{attacker} of nodes in the neighborhood of the other nodes for all t, i.e. $|\mathcal{V}_i[t] \cap \mathcal{S}| \leq f_{\text{attacker}}|\mathcal{V}_i[t]|, \forall i \in \mathcal{V} \backslash S$, $\forall t \in \mathbb{Z}_{\geq 0}, 0 \leq f_{\text{attacker}} \leq 1$.

A group of adversary nodes is considered F-locally bounded or f_{attacker}-*fraction* locally bounded if it forms an F-local set or f_{attacker}-*fraction* local set, respectively. These threat scopes are known as the F-local and f_{attacker}-*fraction* local models. Later, we will use these models, each based on distinct robust properties, to evaluate the effectiveness of our strategy.

Definition 2.4 ((r,s)-Reachable Set, [30]). Given a graph $\mathcal{G}$ and a nonempty subset of nodes $\mathcal{S}$, $\mathcal{S}$ is defined as an (r,s)-reachable set if it encompasses at least s nodes, each maintaining a minimum of r connections with nodes external to $\mathcal{S}$, where $r, s \in \mathbb{Z}_{\geq 0}$; i.e. given $\mathcal{X}_{\mathcal{S}}^r = \{i \in \mathcal{S} : |\mathcal{V}_i \backslash \mathcal{S}| \geq r\}$, then $|\mathcal{X}_{\mathcal{S}}^r| \geq s$.

Definition 2.5 ((r,s)-Robust Graph, [30]). Consider a nonempty, nontrivial directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with N

nodes ($N \geq 2$). $\mathcal{G}$ is termed (r,s)-robust, where nonnegative integers $r \in \mathbb{Z}_{\geq 0}, 1 \leq s \leq N$, if for every pair of nonempty, disjoint subsets $\mathcal{S}_1$ and $\mathcal{S}_2$ of $\mathcal{V}$ at least one of the following holds (recall $\mathcal{X}_{\mathcal{S}_k}^r = \{i \in \mathcal{S}_k : |\mathcal{V}_i \backslash \mathcal{S}_k| \geq r\}$ for $k \in \{1,2\}$):

$$\begin{aligned} &|X_{S_1}^r| = |\mathcal{S}_1|; \\ &|X_{S_2}^r| = |\mathcal{S}_2|; \\ &|X_{S_1}^r| + |X_{S_2}^r| \geq s. \end{aligned} \tag{2}$$

In addition to the previously discussed (r,s)-robust graph, researchers have proposed security conditions tailored to other specific scenarios, as illustrated by the definition provided below.

Definition 2.6 (p-fraction Reachable Set, [30]). Given a graph $\mathcal{G}$ and a nonempty subset $\mathcal{S}$ of nodes of $\mathcal{G}$, $\mathcal{S}$ is designated as a p-*fraction* reachable set if $\exists i \in \mathcal{S}$ such that $|\mathcal{V}_i| > 0$ and $|\mathcal{V}_i \backslash \mathcal{S}| \geq p|\mathcal{V}_i|$, where $0 \leq p \leq 1$. If $|\mathcal{V}_i| = 0$ or $|\mathcal{V}_i \backslash \mathcal{S}| = 0$ for all $i \in \mathcal{S}$, then $\mathcal{S}$ is 0-*fraction* reachable.

Definition 2.7 (p-fraction Robust Graph, [30]). A nonempty, nontrivial graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ comprising N nodes ($N \geq 2$) is classified as p-*fraction* robust, where $0 \leq p \leq 1$, provided that for every pair of nonempty, disjoint subsets of $\mathcal{V}$, at least one subset is p-*fraction* reachable. In the case of an empty or trivial $\mathcal{G}$ (where $N \leq 1$), $\mathcal{G}$ is considered 0-*fraction* robust.

The aforementioned definitions constitute the fundamental aspects of robust graph theory. To provide a more comprehensive explanation of the CBF for constructing (r,s)-robust graphs, as delineated in this study, we propose the following definition.

Definition 2.8 (Osmosis Node). In a simple digraph $\mathcal{G}$, a node fulfilling the subsequent criteria is referred to as an osmosis node:

- Osmosis nodes possess direct edges to every other node within graph $\mathcal{G}$, excluding itself;
- Each remaining node in graph $\mathcal{G}$, apart from itself, contains direct edges to osmosis nodes.

Definition 2.9 (Pure Osmosis Graph). A simple digraph $\mathcal{G}$ is considered a pure osmosis graph if and only if, after removing all osmosis node and their associated edges from the graph $\mathcal{G}$, the graph becomes empty or the residual edge set is $\emptyset$.

Definition 2.10 (Degree of Osmosis). Given a simple digraph, denoted as $\mathcal{G}$, the degree of osmosis can be expressed as $K_{os} = \frac{n_{os}}{N}$, where n_{os} represents the number of osmosis nodes within the graph, while N signifies the total number of nodes present.

Evidently, a graph comprises not only osmosis nodes but also non-osmosis nodes. In other words, when $k_{os} = 0$, it

does not imply that the graph is a scattered graph. Conversely, when $k_{os} = 1$, the graph is a complete graph.

2.2. *Control barrier function*

We consider a control system represented as

$$\dot{\mathbf{x}} = f(\mathbf{x}) + g(\mathbf{x})\mathbf{u}, \qquad (3)$$

where $\mathbf{x} \in \mathcal{D} \subset \mathbb{R}^n, \mathbf{u} \in \mathcal{U} \subset \mathbb{R}^m$, and f and g are Lipschitz continuous. We define the desirable set $\mathcal{C}$ for the system via the continuously differentiable function $h(\mathbf{x})$, represented as

$$\mathcal{C} = \{\mathbf{x} \in \mathbb{R}^n : h(\mathbf{x}) \geq 0\}. \qquad (4)$$

Definition 2.11 (Finite-time Convergence Control Barrier Function, [21]). Consider a dynamical system, as defined in (3), along with the set $\mathcal{C}$ as outlined in (4), defined by a continuously differentiable function $h : \mathcal{R}^n \to \mathcal{R}$. If there exist real parameters $\rho \in [0, 1)$, $\gamma > 0$, and a subset $\mathcal{C} \subseteq \mathcal{D} \subset \mathbb{R}^n$ such that for all $\mathbf{x} \in \mathcal{D}$,

$$\sup_{\mathbf{u} \in \mathcal{U}}[L_f h(\mathbf{x}) + L_g h(\mathbf{x})\mathbf{u} + \gamma \mathrm{sign}(h(\mathbf{x}))|h(\mathbf{x})|^\rho] \geq 0, \qquad (5)$$

where L_f and L_g are the Lie derivative over f and g, respectively, the function h is then classified as a Finite-time Convergence Control Barrier Function (FCBF) defined on the set $\mathcal{D}$.

Given a FCBF h, the set of feasible control inputs is

$$\begin{aligned} K(\mathbf{x}) = \{\mathbf{u} \in \mathcal{U} : L_f h(\mathbf{x}) + L_g h(\mathbf{x})\mathbf{u} \\ + \gamma \, \mathrm{sign}(h(\mathbf{x}))|h(\mathbf{x})|^\rho \geq 0\}. \end{aligned} \qquad (6)$$

Lemma 2.1 ([21]). *Consider a set $\mathcal{C} \subset \mathbb{R}^n$ linked with a FCBF $h(\mathbf{x})$, defined over $\mathcal{D}$ where $\mathcal{C} \subseteq \mathcal{D} \subset \mathbb{R}^n$, and parameters $\rho \in [0, 1)$ and $\gamma > 0$. Any continuous controller $\mathbf{u} : \mathcal{D} \to \mathcal{U}$, satisfying $\mathbf{u} \in K(\mathbf{x})$ for system (3), ensures forward invariance of the set $\mathcal{C}$. Furthermore, given an initial state $\mathbf{x}_0 \in \mathcal{D} \backslash \mathcal{C}$, any such continuous controller drives the state $\mathbf{x}$ to $\mathcal{C}$ within a finite time $T = \frac{1}{\gamma(1-\rho)}|h(\mathbf{x}_0)|^{1-\rho}$.*

Consider a communication graph $\mathcal{G}_k$ that a formation of N nodes must adhere to by time t_k. The edge requirement $(i, j) \in \mathcal{E}_k$ can be encoded in the set $\mathcal{C}_{ij} = \{\mathbf{x} \in \mathbb{R}^{2N} : h_{ij}(\mathbf{x}) \geq 0\}$, where $\mathbf{x} \in \mathbb{R}^{2N}$ is a vector representing the position coordinates of the N nodes, and $h_{ij}(\mathbf{x}) = R^2 - \|\mathbf{x}_i - \mathbf{x}_j\|^2$, where R is communication range. The constraints corresponding to all the pairs in the edge set can be collectively represented in a single set $\mathcal{C}_k = \bigcap_{(i,j) \in \mathcal{E}_k} \mathcal{C}_{ij}$.

According to [21], for a given nominal control input $\hat{\mathbf{u}}_i$ of node i, the control input $\boldsymbol{u}_i$ closest $\hat{\mathbf{u}}_i$ to that best satisfies the constraints can be determined using quadratic

programming as Eq. (7):

$$\mathbf{u}^* = \operatorname*{argmin}_{\mathbf{u}} \sum_{i=1}^N \|\mathbf{u}_i - \hat{\mathbf{u}}_i\|^2 \qquad (7)$$

$$\text{s.t. } \dot{h}_{ij}(\mathbf{x}) + \gamma \mathrm{sign}(h_{ij}(\mathbf{x}))|h_{ij}(\mathbf{x})|^\rho \geq 0.$$

This is a quadratic programming for the control input $\mathbf{u}_i$. Utilizing Eq. (7), we can derive the desired control input. It is important to highlight that the expansion of constraints can be guided by Eq. (5).

The field of obstacle avoidance utilizing control barrier functions has been extensively explored in [20], and the barrier functions developed therein can be seamlessly integrated with our approach. Therefore, in this paper, our primary emphasis lies in highlighting our unique contributions to formations.

3. Enhancing Robustness in Formation

In this section, we first address two key properties of robust formation control problems: (r, s)-robustness and *p-fraction* robustness. We introduce the (r, s)-robustness and present a theorem to determine the required lower bound to achieve this robustness. Furthermore, we explore the *p*-fraction robustness and present a theorem that outlines the necessary conditions to achieve this robustness.

These findings provide a theoretical foundation and guidance for designing control algorithms that ensure stable and efficient formation of multi-UAV systems.

3.1. (r,s)-robust graph

We provide a comprehensive overview of utilizing FCBF to develop a communication topology that satisfies (r, s)-robust properties for a formation. To achieve this goal, pertinent conclusions are discussed.

Theorem 3.1. *If graph $\mathcal{G}$ is a pure osmosis graph, the following conclusions can be drawn:*

- *For graph with an odd number of nodes N, graph $\mathcal{G}$ is n_{os}-robust when $K_{os} \leq \frac{N+1}{2N}$. On the other hand, when $\frac{N+1}{2N} \leq K_{os} < 1$, graph $\mathcal{G}$ satisfies the $\left(\frac{N+1}{2}, n_{os} - \frac{N-1}{2}\right)$-robust.*
- *For graph with an even number of nodes N, graph $\mathcal{G}$ exhibits n_{os}-robust when $K_{os} \leq \frac{1}{2}$ and satisfies the $\left(\frac{N+1}{2}, n_{os} - \frac{N-1}{2}\right)$-robust when $\frac{1}{2} \leq K_{os} < \frac{N-2}{N}$.*

Proof. To provide a clearer exposition of this theorem, the proof is separated into two components. Initially, the r-robustness is demonstrated for degree of osmosis $K_{os} \leq \frac{1}{2}$.

Subsequently, the (r, s)-robustness is established when degree of osmosis $K_{os} > \frac{1}{2}$.

Part 1 Proof: Consider a graph with an odd number N. When $K_{os} \leq \frac{N+1}{2N}$, it follows that $n_{os} \leq \frac{N+1}{2}$. In this case, the nodes in the graph can be classified into two categories: (1) osmosis nodes and (2) non-osmosis nodes. The upper bound of value of r is established by the minimum in-degree of its vertices, which implies that $r_{\max} \leq n_{os}$. To determine the lower bound of $r_{\max}$, we analyze partitioning. Let $\mathcal{P}_k$ denote a vertex subset of size k for the graph $\mathcal{G}_F$, and let (τ_1, τ_2) represent a partition of $\mathcal{P}_k$ that satisfies the following conditions: (1) $|\tau_1| \cdot |\tau_2| \neq 0$, (2) $\tau_1 \cap \tau_2 = \emptyset$ and $\tau_1 \cup \tau_2 = \mathcal{P}_k$, and (3) $\mathcal{R}(\tau_1) \geq \mathcal{R}(\tau_2)$. Here, $\mathcal{R}(\tau) = r$ to the r-robust graph of vertex set τ. We proceed with a proof by contradiction, assuming that the graph's robustness value satisfies $r_{\max} \leq n_{os} - 1$. In that case, a partition must exist such that $\max(\mathcal{R}(\tau_1), \mathcal{R}(\tau_2)) \leq n_{os} - 1$. We discuss $\mathcal{P}_k$ to identify this partition, considering three possible scenarios for $\mathcal{P}_k$.

- Case 1: $\mathcal{P}_k$ solely comprises osmosis nodes;
- Case 2: $\mathcal{P}_k$ lacks any osmosis nodes;
- Case 3: $\mathcal{P}_k$ partially includes osmosis nodes.

In Case 1, for any given pair (τ_1, τ_2), it holds that $\mathcal{R}(\tau_1) > N - n_{os}$ and $\mathcal{R}(\tau_2) > N - n_{os}$. By considering discrete positive integers, we obtain $\mathcal{R}(\tau_1) \geq \frac{N-1}{2} + 1 = \frac{N+1}{2}$. At this stage, the graph reaches its maximum value for this particular number of nodes. Consequently, this partition can only represent the value of r when n_{os} reach the upper bound of $\frac{N+1}{2}$, meaning $\mathcal{R}(\tau_1) \geq \frac{N+1}{2}$;

In Case 2, for any given pair (τ_1, τ_2), the calculation yields $\mathcal{R}(\tau_1) = n_{os}$;

In Case 3, we examine whether τ_1 includes the osmosis nodes and subsequently analyze $\mathcal{R}(\tau_1)$. If τ_1 does not contain the osmosis nodes, then $\mathcal{R}(\tau_1) = n_{os}$. Conversely, if τ_1 comprises the osmosis nodes, we evaluate the scenario where $\mathcal{R}(\tau_1) \leq n_{os} - 1$, ensuring $\mathcal{R}(\tau_1) \geq \mathcal{R}(\tau_2)$. To accomplish this, the external neighbors of osmosis nodes must be fewer than n_{os}, and it is necessary to ascertain $|\tau_1| \geq N - n_{os} + 1$, thus implying $|\tau_2| \leq n_{os} - 1$. In this case, $\mathcal{R}(\tau_2) \geq n_{os}$, violating the condition $\mathcal{R}(\tau_1) \geq \mathcal{R}(\tau_2)$. Consequently, the graph's lower bound of $r_{\max}$ is n_{os}, meaning $r_{\max} \geq n_{os}$. Coupled with the previously established inequality, $r_{\max} \leq n_{os}$, we deduce $r_{\max} = n_{os}$. For graphs with even N, when $K_{os} \leq \frac{1}{2}$, $n_{os} \leq \frac{N}{2}$, and the proof procedure parallels that of graphs with odd N. Hence, the first part is substantiated.

Part 2 Proof. Considering the graph's maximum achievable robustness value of $r_{\max} \leq \lfloor \frac{n+1}{2} \rfloor$ and the fact that adding edges does not reduce the value of r, the (r, s)-robustness proof for the graph focuses solely on the value of s when the degree of osmosis $K_{os} > \frac{1}{2}$.

For a graph with an odd number N, when $K_{os} \geq \frac{N+1}{2N}$, it follows that $n_{os} \geq \frac{N+1}{2}$. According to the theorem, the maximum value of r is given by $r_{\max} = \frac{N+1}{2}$. Consequently, it is necessary to examine partitions of the set based on the number of nodes with a minimum of $\frac{N+1}{2}$ external neighbors. The vertex subset $\mathcal{P}_k$ of the graph $\mathcal{G}_F$ has a size of k, and (τ_1, τ_2) constitutes a partition of $\mathcal{P}_k$ under the conditions: (1) $|\tau_1| \neq 0$ and $|\tau_2| \neq 0$; (2) $\tau_1 \cap \tau_2 = \emptyset$ and $\tau_1 \cup \tau_2 = \mathcal{P}_k$; (3) $|\tau_1| > |\tau_2|$. In this context, χ_τ^r denotes the set of nodes in the set τ with at least r external neighbors. It is noteworthy that this section consistently relies on the premise of $r = r_{\max}$. Based on the definition of the value s, it is evident that $|\tau_1| > |\chi_{\tau_1}^r|$ and $|\tau_2| > |\chi_{\tau_2}^r|$. Thus, both sets must contain a minimum of 1 node with external neighbors fewer than $r_{\max}$, implying that $|\mathcal{P}_k| \geq 3$. Given $d = n_{os} - \frac{N+1}{2} + 1 = n_{os} - \frac{N-1}{2}$, the graph exhibits $(\frac{N+1}{2}, d)$-robustness, where d symbolizes the number of penetration nodes in the graph more than $\frac{N-1}{2}$.

When $n_{os} = \frac{N+1}{2}$, we deduce that $d = 1$. Also, given $1 \leq s \leq N$, the lower bound for s is 1. Furthermore, a partition exists where $|\mathcal{P}_k| = N, \tau_1 = \mathcal{P}_k - \tau_2, \tau_2 = \{\text{node}_{os \cdot 1}, \text{node}_{os \cdot 2}, \ldots, \text{node}_{os \cdot (r-1)}, \text{node}_{\text{non-}os \cdot 1}\}$, where $\text{node}_{os \cdot i}$ represents the ith osmosis node, $\text{node}_{\text{non-}os \cdot 1}$ is the non-osmosis node, and in which the outcome derived from this partition yields $s = 1$. Therefore, it satisfies $s = d$ in this case.

When $n_{os} > \frac{N+1}{2}$, we first determine an upper bound for s using set partitioning and subsequently prove that a partition with a lower value of s cannot be attained, thus establishing the lower bound. A partition exists where $|\mathcal{P}_k| = N, \tau_1 = \mathcal{P}_k - \tau_2$, and $\tau_2 = \{\text{node}_{os \cdot 1}, \text{node}_{os \cdot 2}, \ldots, \text{node}_{os \cdot (\frac{N-1}{2} - 1)}, \text{node}_{\text{non-}os \cdot 1}\}$, such that this partition results in $s = d$, offering an upper bound for s. For analyzing the lower bound of s, we consider three potential scenarios for $\mathcal{P}_k$:

- Case 1: $\mathcal{P}_k$ contains exclusively osmosis nodes;
- Case 2: $\mathcal{P}_k$ includes no osmosis nodes;
- Case 3: $\mathcal{P}_k$ partially comprises osmosis nodes.

In Case 1, for any given pair (τ_1, τ_2), considering $|\tau_1| + |\tau_2|$, it becomes infeasible for both sets to simultaneously contain at least one node failing to meet the requirement of possessing an external neighbor greater than or equal to $r_{\max}$.

In Case 2, given that $|\mathcal{P}_k| < \frac{N-1}{2}$, neither (τ_1, τ_2), nor any pair thereof, can ensure that a minimum of one node per set satisfies the condition whereby its external neighbors are greater than or equal to $r_{\max}$.

In Case 3, we examine whether τ_1 includes the osmosis nodes. If τ_1 does not comprise the osmosis nodes, all external neighbors of nodes within τ_1 are greater than or equal to $r_{\max}$. Consequently, the partition condition is

unmet. On the other hand, when τ_1 contains the osmosis nodes, τ_2 must also include the osmosis nodes; otherwise, all external neighbors of nodes in τ_2 are greater than or equal to $r_{\max}$. We employ the contradiction method, presuming the graph has $s \leq d - 1$. In this case, there must exist a partition for which $\left| \chi_{\tau_1}^r \right| + \left| \chi_{\tau_2}^r \right| \leq d - 1$. We need to discuss $|\mathcal{P}_k|$ here: when considering $|\mathcal{P}_k|$, there must be either n_{os} nodes or $N - n_{os}$ nodes outside $\mathcal{P}_k$. For a partition fulfilling the requirements, i.e. both sets have at least 1 node that does not meet the external neighbors being greater than or equal to $r_{\max}$, add the nodes outside $\mathcal{P}_k$ to the larger set in (τ_1, τ_2). Doing so will neither change the number of nodes in the smaller set with external neighbors greater than or equal to $r_{\max}$ nor increase the number of nodes in the smaller set with external neighbors greater than or equal to $r_{\max}$. Thus, the final discovered partition may be equivalent to $|\mathcal{P}_k| = N$, with both (τ_1, τ_2) containing osmosis nodes. We now need to analyze this scenario.

Since $|\tau_1| > |\tau_2|$, $|\chi_{\tau_1}^r| = 0$, the minimum value of $|\chi_{\tau_2}^r|$ represents the lower bound of s. It is evident that the external neighbors of the osmosis nodes in τ_2 are greater than or equal to $r_{\max}$. This is equivalent to attempting to minimize the number of osmosis nodes in τ_2, and the amount of external neighbors for the non-osmosis nodes is less than $r_{\max}$. The number of external neighbors for the non-osmosis nodes consistently changes and can only satisfy that there are at most $r_{\max} - 1$, which is $\frac{N-1}{2}$ osmosis nodes in τ_1. At this juncture, the number of osmosis nodes in τ_2 is minimized, equating to $n_{os} - \frac{N-1}{2} = d$. This proves that no such partition exists, such that $|\chi_{\tau_1}^r| + |\chi_{\tau_2}^r| \leq d - 1$, meaning the lower bound of s exists, and the lower bound is $s \geq d$, and $s = d$ as evidenced.

In a graph with an even number of nodes N and $K_{os} \geq \frac{1}{2}$, $n_{os} \geq \frac{N}{2}$. During the partitioning process, situations may arise where $|\tau_1| = |\tau_2|$. For the partition (τ_1, τ_2) in Case 3, it is evident that both sets possess node counts contributing to the final s value, precluding the occurrence of the smallest s partition. Consequently, such cases may be disregarded to explore the potential for a smaller value of s. The remainder of the proof aligns with graphs containing an odd number of nodes, thereby concluding the proof.   □

Based on the aforementioned proof, it becomes apparent that the process of ascertaining the number of osmosis nodes within the topological structure holds the key to establishing and guaranteeing the (r, s)-robustness of the system. Consequently, the manipulation and oversight of the proliferation of osmosis nodes within this topological framework plays a pivotal role in the regulation of the system (r, s)-robustness. Section 4 shall comprehensively elucidate the intricate nuances of this control algorithm.

3.2.   *p-fraction robust graph*

The application of FCBF for constructing a topology that satisfies the requirements of a *p-fraction* robust graph for formation is presented. Theorem 3.2 delineates the essential properties a topology should exhibit to satisfy the *p-fraction* robust graph.

Theorem 3.2. *A graph $\mathcal{G}$ with N nodes is considered a p-fraction robust graph if it satisfies the following conditions:*

- *Within a set $\mathcal{S}$ of $N(1 - p)$ nodes, where $p = \frac{k}{N}$ and $k \in \{0, 1, \ldots, N\}$, it holds that $\mathcal{V}_i \leq n_{\mathrm{neigh}} < N, i \in \mathcal{S}$;*
- *The remaining Np nodes are fully connected to all other nodes in the graph.*

Then, the graph $\mathcal{G}$ is a p-fraction robust graph, and the value of $p \geq \min\{\frac{N/2}{N-1}, \frac{k}{n_{\mathrm{neigh}}}\}$.

Proof. Let $\mathcal{S}_k$ denote a subset comprising k nodes, each connected to every other node, and let $\mathcal{S}_{N-k}$ represent the remaining $N - k$ nodes in the subset. Furthermore, define non-empty and disjoint subsets, $\mathcal{S}_1$ and $\mathcal{S}_2$, of V such that $|\mathcal{S}_1| \leq |\mathcal{S}_2|$.

Consider node $i \in \mathcal{S}_1$, and assume that $\mathcal{S}_1 \cap \mathcal{S}_k \neq \emptyset$ and node $i \in \mathcal{S}_1 \cap \mathcal{S}_k$. From this, we can deduce that $|V_i| = N - 1$ and $|V_i \setminus \mathcal{S}_1| = (N - 1) - (|\mathcal{S}_1| - 1) \geq \frac{N}{2}$. Clearly, $\frac{|V_i \setminus \mathcal{S}_1|}{|V_i|} \geq \frac{N/2}{N-1}$, signifying that $\mathcal{S}_1$ is a *p-fraction* set with $p \geq \frac{N/2}{N-1}$.

When assuming $\mathcal{S}_1 \cap \mathcal{S}_k = \emptyset$, we can infer that $\mathcal{S}_1 \subset \mathcal{S}_{n-k}$. Following the previous topological construction, any node in $\mathcal{S}_1$ is connected to k nodes in $\mathcal{S}_k$. Consequently, the number of external neighbors $|V_i \setminus \mathcal{S}_1| \geq k$. Given that the condition stipulates the number of neighbors in $\mathcal{S}_{N-k}$ cannot exceed n_{neigh}, it can be deduced that $|V_i| \leq n_{\mathrm{neigh}}$ and $\frac{|V_i \setminus \mathcal{S}_1|}{|V_i|} \geq \frac{k}{n_{\mathrm{neigh}}}$. Thus, $\mathcal{S}_1$ is indeed a *p-fraction* set with $p \geq \frac{k}{n_{\mathrm{neigh}}}$.

In conclusion, regardless of whether a node in $\mathcal{S}_1$ is in $\mathcal{S}_k$, $\mathcal{S}_1$ always remains a *p-fraction* set. Therefore, the constructed graph $\mathcal{G}$ is a *p-fraction* robust graph, with $p \geq \min\{\frac{N/2}{N-1}, \frac{k}{n_{\mathrm{neigh}}}\}$.   □

As long as the conditions described in Theorem 3.2 are satisfied, we can obtain a *p-fraction* robust graph. To achieve this, we construct the function S_{ij} with the following properties, and δ_{ij} represents the distance between node i and j:

(a) S_{ij} belongs to the C^1 class, making it a continuously differentiable function;
(b) $S_{ij}(0) < 0, S_{ij}(R) = 0$. When $\mu R \leq \delta_{ij} \leq \delta_{\max}, 1 < \mu < \frac{\delta_{\max}}{R}$, $S_{ij}(\delta_{ij}) = -(N - 2)S_{ij}(0)$;
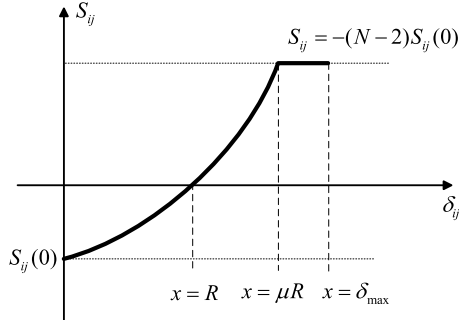(c) S_{ij} is strictly increasing when $0 < \delta_{ij} \leq \mu R$;
(d) For $\delta_{ij} = 0, \frac{dS_{ij}}{d\delta_{ij}} > 0$.

Fig. 1.   Graph of the function S_{ij} satisfying properties (a) to (d) used in our paper. As the distance δ_{ij} between nodes i and j increases, S_{ij} also gradually increases. However, for the sake of computational simplicity, we have set a maximum distance value, denoted as $\delta_{\max}$. Any distances greater than $\delta_{\max}$ are considered equal to $\delta_{\max}$. Additionally, we define $S_{ij}(\delta_{ij}) = -(N-2)S_{ij}(0)$ as our expected result.

Based on these four properties (a)–(d), we can obtain a function, as depicted in Fig. 1, which serves as a constraint on the distances between nodes.

For ease of comprehension, the following definitions are provided:

$$m = S_{ij}(0), \tag{8}$$

$$M = -(N-2)S_{ij}(0), \tag{9}$$

$$S_i = \sum_{j \in \mathcal{V}\backslash\{i\}} S_{ij}. \tag{10}$$

To further elucidate our work, Theorem 3.3 delineates the constraints pertaining to the upper bound on the number of neighboring nodes.

Theorem 3.3. *Given a set $\mathcal{V}$ with $N > 2$ nodes and a function S_{ij} that fulfills conditions (a)–(d), let S_i be defined as in the preceding Eq. (10). If $1 \leq n_p \leq N-1$, and $S_i \geq (N - n_p - 1)M$, a maximum of n_p neighbors can be found within the communication range R of node i.*

Proof. Consider the set of neighbors within communication range R of node i, denoted as $\mathcal{V}_i$, such that $0 \leq |\mathcal{V}_i| \leq N-1$. The function S_i can be decomposed into the following equation:

$$S_i = \sum_{j \in \mathcal{V}\backslash\{i\}} S_{ij} = \sum_{j \in \mathcal{V}_i} S_{ij} + \sum_{j \in \mathcal{V}\backslash(\mathcal{V}_i \cup \{i\})} S_{ij}. \tag{11}$$

If node j is the neighbor of node i, the value of S_i falls within the range $(m, 0]$. Conversely, if node j is not the neighbor of node i, the value of S_i ranges from $(0, M]$. Given that the number of node i non-neighbors is in the range $0 \leq |\mathcal{V}\backslash\mathcal{V}_i| \leq N-2$, we can determine the upper bound of S_i such that $S_i < |\mathcal{V}\backslash\mathcal{V}_i|M$. We set $S_{ij}(\delta_{ij}) = -(N-2)S_{ij}(\delta_{\max})$ to ensure the inequality remains valid when there is only 1 neighbor.

Based on the condition, $S_i \geq (N - (n_p - 1))M$. Therefore, we deduce that

$$(N - (n_p - 1))M \leq S_i < |V\backslash\mathcal{V}_i|M, \tag{12}$$

which can be simplified to

$$(N - n_p - 1) < |V\backslash\mathcal{V}_i|. \tag{13}$$

As the number of nodes takes discrete integer values, the number of node i non-neighbors is at least $N - n_p$, indicating that there can be no more than n_p neighbors.   □

Based on the aforementioned Theorem 3.3, we can limit the number of neighbors for node i. Nonetheless, our ultimate objective is to create a *p-fraction* robust graph. To approach this goal, we establish the function $\mathfrak{f}$, with its corresponding relationship function depicted in Fig. 2. This function consists of the following properties:

(i) $\mathfrak{f}$ is a C^1 class, continuously differentiable function.
(ii) $\mathfrak{f}((N-1)m) < 0$. $\mathfrak{f}((N-n_p-1)M) = 0$, and for $(N-n_p-1+\alpha)M \leq S_i \leq (N-1)M$ with $0 < \alpha < 1$, $\mathfrak{f}(S_i) = -(N-1)\mathfrak{f}((N-1)m)$.
(iii) $\mathfrak{f}$ is strictly increasing when $(N-1)m \leq S_i < (N - n_p - 1 + \alpha)M$.

For ease of comprehension, the following definitions are provided:

$$a = \mathfrak{f}((N-1)m), \tag{14}$$

$$A_p = -(N-1)\mathfrak{f}((N-1)m), \tag{15}$$

$$S_p = \sum_{i \in V} \mathfrak{f}(S_i). \tag{16}$$

Based on function $\mathfrak{f}$, the following theorem is derived.

Theorem 3.4. *Let $\mathcal{V}$ be a set of $N > 2$ nodes, for $1 \leq n_p \leq N-1$ and $1 \leq k_p \leq N$, if $S_p \geq (k_p - 1) A_p$, then the communication range R of at least k_p nodes contains a maximum of n_p neighbors.*
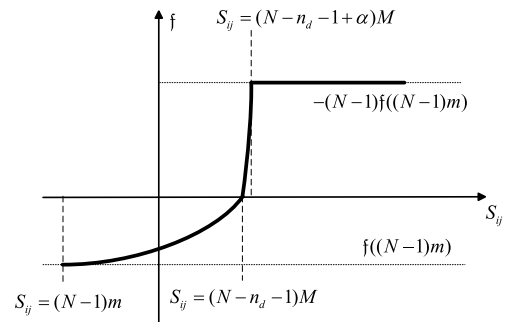

Fig. 2.   Graph of the function $\mathfrak{f}$ satisfying properties (i) to (iii) used in our paper. We define $\mathfrak{f}(S_{ij}) = -(N-1)\mathfrak{f}((N-1)m)$ as our expected result.

Proof. Let $\mathcal{A}$ represent the set of all nodes i such that $S_i \geq (N - n_p - 1)M$. Based on the previous theorem, the number of neighbors within the communication range R not exceeding n_p is denoted by $|\mathcal{A}|$.

Given the above definition, when node j is a neighbor of node i, the value range of S_{ij} is $(m, 0]$, whereas if node j is not a neighbor of node i, the value range of S_i is $(0, M]$. For $i \in \mathcal{A}$, the range of S_i becomes $[(N - n_p - 1)M, (N - 1)M]$, and for $i \in \mathcal{V} \backslash \mathcal{A}$, the range of S_i is $((N - 1)m, (N - n_p - 1)M)$. Subsequently, the function $\mathfrak{f}$ maps these intervals to $(0, A)$ and $[a, 0)$, allowing the calculation of the value of S as follows:

$$S = \sum_{i \in \mathcal{V}} \mathfrak{f}(S_i) = \sum_{i \in \mathcal{A}} \mathfrak{f}(S_i) + \sum_{i \in \mathcal{V} \backslash \mathcal{A}} \mathfrak{f}(S_i). \qquad (17)$$

Consequently, the upper limit can be expressed as

$$S_p < |\mathcal{A}| A_p. \qquad (18)$$

Considering the stated assumption, $S_p \geq (k_p - 1)A_p$ holds true for $1 \leq k_p \leq N$ and $1 \leq n_p \leq N - 1$. The subsequent inequality is derived as follows:

$$(k_p - 1)A_p \leq S_p < |\mathcal{A}| A_p. \qquad (19)$$

As a result, $k_p - 1 < |\mathcal{A}|$, and since k_p and $|\mathcal{A}|$ represent discrete values, it follows that $|\mathcal{A}| \geq k_p$. Thus, there are at least k_p nodes with no more than n_p neighbors in the range R. □

As stated in Theorem 3.4, a minimum of k_p nodes can be controlled to ensure that the number of neighboring nodes within the range R remains below n_p.

4.   Robust Formation Construction

The preceding section primarily delved into the properties required to satisfy robust graph as outlined in Theorems 3.1 and 3.2. Furthermore, in Theorems 3.3 and 3.4, the method for constructing a *p-fraction* robust graph was explicated. It is imperative to note that we abstained from the development of (r, s)-robust graphs, as pertinent theorems pertaining to this were rigorously addressed in [23]. In this section, we shall expound upon the utilization of the FCBF for the construction of the robust graphs.

4.1.   *Enforcing* **(r,s)**-*robust formation*

The proof of Theorem 3.1 indicates that if the given conditions are satisfied, an (r, s)-robust graph satisfying the lower bound can be constructed. However, the construction method for such a graph is not explicitly detailed in the text.

In literature [23], a formation control strategy is proposed to ensure that at least k_d nodes have at least n_d neighbors within the communication range R. Inspired by [23], we further utilize this strategy to present a formation algorithm for constructing (r, s)-robust networks in this paper.

Lemma 4.1 ([23]). *If a set $\mathcal{V}$ with $N > 2$ nodes, for $1 \leq n_d \leq N - 1, 1 \leq k_d \leq N$, if $S_{rs} \geq (k_d - 1)A_{rs}$, then there exist at least k_d nodes within the communication range R having at least n_d neighbors. Here, n_d denotes the number of neighbors for a node, k_d signifies the number of such nodes, while S_{rs} and A_{rs} represent the current optimization value and the target optimization value, respectively. And FCBF can enforce the formation communication with r-robustness in finite time.*

By utilizing the method proposed in Lemma 4.1, we can adjust the parameters to obtain the desired result stated in Theorem 3.1, namely, the construction of an (r, s)-robust graph that satisfies the lower bound. For further details, see [23]. The specific parameter settings are illustrated in Eq. (20). By ensuring the presence of a sufficient number of osmosis nodes, it is possible to construct a communication topology that fulfills the lower bound for an (r, s)-robust graph.

$$h_{rs}(\mathbf{x}) = S_{rs} - (k_d - 1)A_{rs}, \qquad (20)$$

where S_{rs} and A_{rs} are defined by Lemma 4.1.

The desired target set is depicted in Eq. (21).

$$\mathcal{C}_{rs} = \{\mathbf{x} \in \mathbb{R}^n : S_{rs} \geq (k_d - 1)A_{rs}\}. \qquad (21)$$

Hence, FCBF can be utilized to construct an eligible (r, s)-robust graph, as demonstrated in Theorem 3.1.

Theorem 4.1. *Let $\mathcal{V}$ be a set of N nodes, where each node has a communication range of R. Given that the controller $\mathbf{u}(\mathbf{x})$ satisfies*

$$\mathbf{u}(\mathbf{x}) \in \{\mathbf{u} \in \mathbb{R}^{2N} : \dot{h}_{rs}(\mathbf{x}) $$
$$ + \gamma \text{sign}(h_{rs}(\mathbf{x}))|h_{rs}(\mathbf{x})|^\rho \geq 0\} := U_{rs}, \qquad (22)$$

where $h_{rs}(\mathbf{x})$ is given by Eq. (20), setting $\rho \in (0, 1), \gamma > 0, n_d = N - 1$, and $k_d = 2s$ ensures that a $(2F + 1, s)$-robust graph satisfying the given condition is obtained within the finite time $T = \frac{1}{\gamma(1-\rho)}|h(\mathbf{x}_0)|^{1-\rho}$, with $s \geq r - \lfloor \frac{N-1}{2} \rfloor$.

Proof. By Lemma 2.1, the set $\mathcal{C}_{rs}$ ensures both attractiveness and forward invariance within a finite time frame. As per Lemma 4.1, this set is representative of a formation encompassing a minimum of $k_d = 2(\lfloor \frac{N}{2} \rfloor - \lfloor \frac{N-1}{2} \rfloor)$ nodes within the communication range of $n_d = N - 1$ nodes. Based on Theorem 3.1, the resulting formation corresponds to a $(\lceil \frac{N}{2} \rceil, s)$-robust graph, with $s \geq r - \lfloor \frac{N-1}{2} \rfloor$. □

The pseudocode of the algorithm is in Algorithm 1.

Algorithm 1   Robust Formation Control with FCBF for (r, s)-Robustness

---
    Input: All nodes position $x \in \mathbb{R}^{2N}$; T represents the duration of system operation; U_{rs} is a set representing all possible control input at one step.

    Output: All nodes position $x \in \mathbb{R}^{2N}$ that satisfies (r, s)-robustness.

  1) $t = 0$
  2) $f(x)$ is the zero matrix, $g(x)$ is the identity matrix
/* Use a simple model to better describe algorithm. */
  3)   With only one constraint, U_{rs} is the set of Eq. (22)
/* The calculation of the variables involved is as mentioned above. You need to adjust the communication range R to change the density of the formation, and k_d to adjust the robustness of the formation. */
  4) **while** $t \leq T$
  5) $u_{min} = u_{max}$ /* Whenever a new u_{min} is computed, it necessitates the recalculation of the set U_{rs} resulting in a relatively substantial computational load. */
  6)   **for** u range in U_{rs}
  7)   **if** $|u|^2 < |u_{min}|^2$
  8) $u_{min} = u$
  9)   **end if**
 10)   Update position $\dot{x} = f(x) + g(x)u_{min} = u_{min}$
 11) $t = t + 1$
 12)   **end for**
 14) **end while**
 15) **Result:**   Final position x

4.2. *Enforcing p-fraction robust formation*

From Theorem 3.2, it is evident that the *p-fraction* robust graph should consist of both k_p nodes with no more than n_p neighbors and k_d osmosis nodes. While the former can be achieved through Theorems 3.3 and 3.4, the latter can be realized through the application of Lemma 4.1.

To ensure the presence of k_p nodes with no more than n_p neighbors in the graph, we construct the following function:

$$h_p(\mathbf{x}) = S_p - (k_p - 1)A_p, \tag{23}$$

where A_p and S_p is defined as Eqs. (15) and (16).

We define the desired set as (24)

$$\mathcal{C}_p = \{\mathbf{x} \in \mathbb{R}^n : S_{rs} \geq (k_d - 1)A_{rs}$$
$$\&\& S_p \geq (k_p - 1)A_p\}, \tag{24}$$

where $k_d + k_p = N$. The first term ensures the existence of k_d osmosis nodes, while the second term ensures the presence of k_p nodes with no more than n_p neighbors, thus meeting the requirements of a *p-fraction* robust graph as stipulated in Theorem 3.1.

However, it is important to note that Eq. (24) indicates the need to construct an law that simultaneously satisfies

both the first and the second term. Therefore, in this paper, a quadratic programming is employed to establish a control strategy that fulfills both conditions concurrently. The QP formulation is detailed in Eq. (7).

Theorem 4.2. *For a system with N nodes, each node has a communication range of R. The controller* $\mathbf{u}(\mathbf{x})$ *satisfies the following conditions:*

$$\mathbf{u}(\mathbf{x}) \in \{\mathbf{u} \in \mathbb{R}^{2N} : \dot{h}_{rs}(\mathbf{x}) + \gamma \mathrm{sign}(h_{rs}(\mathbf{x}))|h_{rs}(\mathbf{x})|^{\rho} \geq 0$$
$$\&\& \dot{h}_p(\mathbf{x}) + \gamma \mathrm{sign}(h_p(\mathbf{x}))|h_p(\mathbf{x})|^{\rho} \geq 0\} := U_p. \tag{25}$$

Given that $h_p(\mathbf{x})$ is as defined in Eq. (23), and given the parameters $\rho \in (0, 1)$, $\gamma > 0$, $n_p = n_{\mathrm{neigh}}$, $k_p = N(1 - p)$, $n_d = N - 1$, and $k_d = Np$, a p-fraction robust graph can be achieved in a finite time $T = \frac{1}{\gamma(1-\rho)}|h(\mathbf{x}_0)|^{1-\rho}$, where $p \geq \min\left\{\frac{N/2}{N-1}, \frac{k}{n_{\mathrm{neigh}}}\right\}$.

Proof. By Lemma 2.1, both finite-time convergence and forward invariance of the set $\mathcal{C}_p$ have been ensured. This set is related to a formation consisting of at least $k_p = N(1 - p)$ nodes with no more than $n_p = n_{\mathrm{neigh}}$ neighbors, and at least $k_d = Np$ nodes with more than $n_d = N - 1$ neighbors. Considering Theorems 3.3 and 3.4, the resulting formation is found to be associated with a *p-fraction* robust graph, where $p \geq \min\{\frac{N/2}{N-1}, \frac{k}{n_{\mathrm{neigh}}}\}$. $\square$

Algorithm 2   Robust Formation Control with FCBF for *p-fraction* Robustness

---
    Input: All nodes position $x \in \mathbb{R}^{2N}$; T represents the duration of system operation; U_p is a set representing all possible control input at one step.

    Output: All nodes position $x \in \mathbb{R}^{2N}$ that satisfies *p-fraction* robustness.

  1) $t = 0$
  2) $f(x)$ is the zero matrix, $g(x)$ is the identity matrix
  3)   By utilizing quadratic programming, integrate two constraints, U_p is the set of Eq. (25) /* Different from (r, s)-robust, *p-fraction* robust requires both fully connected nodes and nodes with an upper bound on the number of neighbors. */
  4) **while** $t \leq T$
  5) $u_{min} = u_{max}$
  6)   **for** u range in U_p /* Change the robustness of the formation by adjusting k_d and k_p. */
  7)   **if** $|u|^2 < |u_{min}|^2$
  8) $u_{min} = u$
  9)   **end if**
 10)   Update position $\dot{x} = f(x) + g(x)u_{min} = u_{min}$
 11) $t = t + 1$
 12)   **end for**
 14) **end while**
 15) **Result:**   Final position x

The key steps of the algorithm are summarized as pseudo-code in Algorithm 2.

5.   Simulation Example

In this section, we present numerical results to demonstrate the effectiveness of our theoretical findings. In particular, we consider a formation swarm composed of seven UAVs moving in a two-dimensional plane. Each UAV is modeled with $\dot{\mathbf{x}} = f(\mathbf{x}) + g(\mathbf{x})\mathbf{u}$. In order to better illustrate the contribution of this paper, we set $f(x)$ to the 0 matrix and $g(x)$ to the identity matrix. The initial positions of the UAVs within a 16×16 units space are shown in Fig. 3. The communication range R around each UAV is represented by a circle, with snowflakes depicting the UAVs. To ensure the accuracy and reproducibility of the simulation, we have meticulously documented all parameters employed in the simulation. The information pertaining to these parameters has been organized in Table 1 for clarity.

We will conduct simulations to verify the robust formation construction strategies mentioned in this article. First, we construct an (r, s)-robust formation that satisfies the lower bounds, as proposed in Theorem 4.1. Then, we
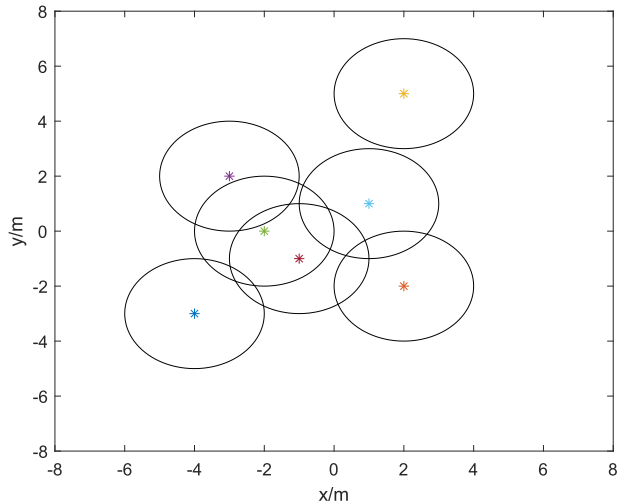
Fig. 3.   Initial position of seven UAVs and each circle represents the communication range of each UAV.

Table 1.   System parameters.

N	R	n_d	k_d	n_{neigh}	k
7	4	6	5	5	5

build a *p-fraction* robust formation that meets the lower bound outlined in Theorem 4.2.

5.1.   (*r,s*)-*robust formation*

To construct a communication graph with $r = r_{\max} = 4$ and $s = s_{\max} = 2$ for a formation consisting of seven UAVs, we can set $n_d = 6$ and $k_d = 5$ based on Theorem 4.1. By applying the controller (22) along with the specified parameters, the nominal formation controller, defined as (26), can be utilized, leading to the construction of a $(4, 2)$-robust formation.

$$\mathbf{u}^* = \underset{\mathbf{u}}{\operatorname{argmin}} \sum_{i=1}^{N} \|\mathbf{u}_i - \hat{\mathbf{u}}_i\|^2 \tag{26}$$

$$\text{s.t. } \dot{h}_{rs}(\mathbf{x}) + \gamma \operatorname{sign}(h_{rs}(\mathbf{x}))|h_{rs}(\mathbf{x})|^\rho \geq 0.$$

The initial positions of seven UAVs are randomly assigned as $(-4, -3)$, $(2, -2)$, $(2, 5)$, $(-3, 2)$, $(-2, 0)$, $(1, 1)$, and $(-1, -1)$ as shown in Fig. 3. In this simulation, we use the ODE function nested with the fmincon function to obtain the update trajectories displayed in Fig. 4 and the update state of r and s displayed in Fig. 5. The four subplots in Fig. 4 illustrate the positions of UAVs in the system at specific values of r and s. The position changes captured by these subplots indicate the robustness of the system with respect to UAVs movements. As the UAVs approach each other, the number of neighbors for each UAV gradually approaches the predetermined number set by the controller (22), leading to an increasing value of r. However, increasing the value of s becomes more challenging, as evident from the trend depicted by the orange line in Fig. 5. Figure 4 displays the communication range after the movement of each UAV using the designed controller. It can be observed that when r is set to 4 and s to 2, the number of neighbors for each UAV meets expectations.

The observations in Figs. 7 and 8 indicate that in situations where a UAV is quite far away from its counterpart, the control input is enhanced to accelerate the shortening of the distance between the UAVs. Conversely, as the distance between UAVs decreases, a reduction in control input is necessary. This modulation of the control input continues until the distance between the UAVs is sufficiently reduced to facilitate the construction of a qualified (r, s)-robust graph. The gradual reduction in control input reflects an adaptive strategy aimed at achieving the desired robust formation with optimal efficiency, emphasizing the system's ability to dynamically adjust to different spatial configurations.

Next, we proceed to randomly designate one UAV as a malicious attacker and demonstrate the convergence of the cluster with the $(4, 2)$-robust formation constructed by
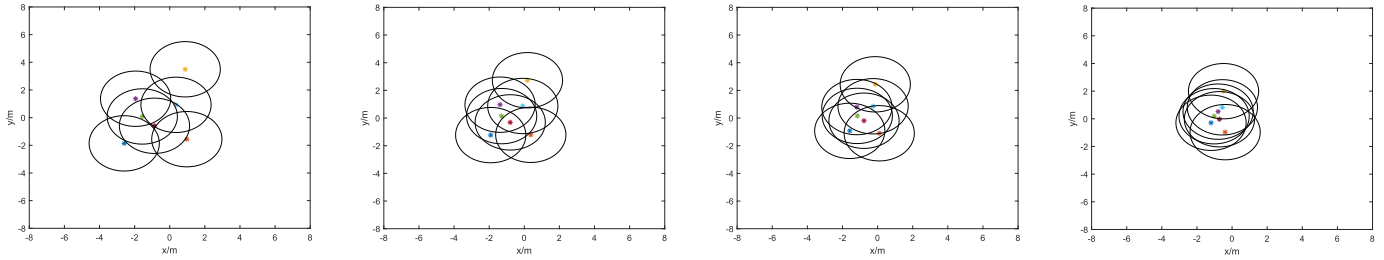
Fig. 4. Position of seven UAVs in the plane. UAVs are represented by snowflakes, while each UAV is represented by the same color. The circle indicates the range of action of each UAV. The robust values from left to right are $(0,7), (1,4), (2,2), (4,2)$.
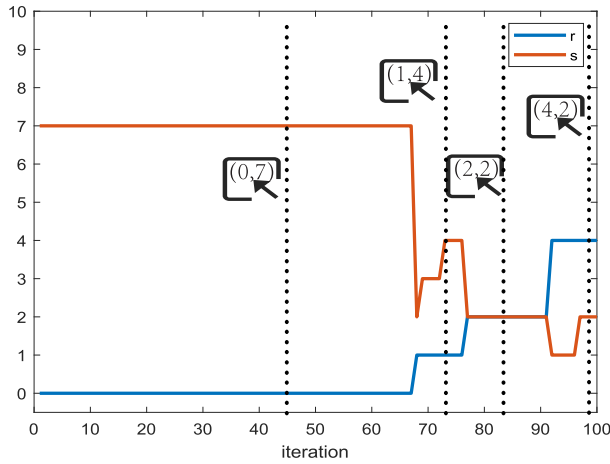

Fig. 5. The trend graph for the values of r and s is represented. The four boxes correspond to the four positions in Fig. 4, each showing the values of r and s.
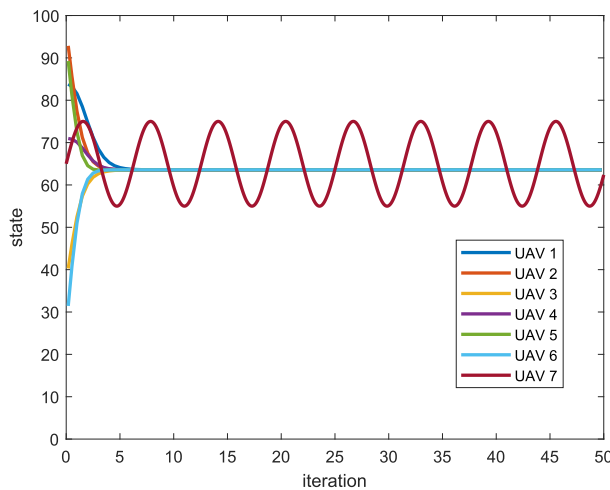

Fig. 7. This graph shows the trend of changes for control input in x when the UAV cluster constructs a (r,s)-robust formation.

Fig. 8. This graph shows the trend of changes for control input in y when the UAV cluster constructs a (r,s)-robust formation.

Theorem 4.1. As depicted in Fig. 6, we initialize the state values of each UAV randomly and designate UAV 7 as the malicious attacker, sending interference values to the other UAVs in the form of a sine curve. It is evident from Fig. 6 that despite the presence of the malicious attacker in the cluster, the formation ultimately achieves resilient consensus. This underscores the efficacy of the proposed control strategy in successfully mitigating the influence of malicious attackers.

5.2. *p-fraction robust formation*

Likewise, by employing the controller (25) mentioned in Theorem 4.2, we can verify whether it constructs a *p-fract ion* robust formation that satisfies the lower bound. Here, we set the parameter $k = 5$ and $n_{\text{neigh}} = 5$. It means that there are five UAVs connected to others and two UAVs with no more than five neighbors. According to Theorem 3.2 and
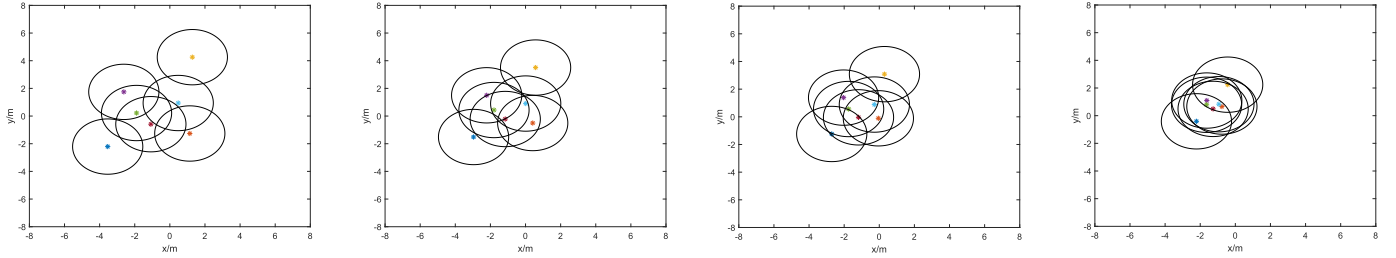

Fig. 6. Consensus diagram depicts a scenario in which UAV 7 acts as a malicious attacker, indicating that each UAV in the system can resist 1 attacker, that is, the other six UAVs can still reach a resilient consensus despite being interfered with.

Fig. 9.   Position of seven UAVs in the plane. UAVs are represented by snowflakes, while each UAV is represented by the same color. The circle indicates the range of action of each UAV. The robust values from left to right are $0, 0.67, 0.76, 1.0$.

the controller (27), we can ensure that the system's robustness reaches at least 7/12.

$$
\mathbf{u}^* = \underset{\mathbf{u}}{\arg\min} \sum_{i=1}^{N} \|\mathbf{u}_i - \hat{\mathbf{u}}_i\|^2,
$$

$$
\text{s.t.} \begin{cases} \dot{h}_{rs}(\mathbf{x}) + \gamma \text{sign}(h_{rs}(\mathbf{x}))|h_{rs}(\mathbf{x})|^\rho \geq 0, \\ \dot{h}_p(\mathbf{x}) + \gamma \text{sign}(h_p(\mathbf{x}))|h_p(\mathbf{x})|^\rho \geq 0. \end{cases} \tag{27}
$$

Then, we use the same initial positions as shown in Fig. 3 and utilize Algorithm 2 to obtain the updated positions, as illustrated in Fig. 9. The four subplots in Fig. 9 depict the positions of UAVs for different values of *p*, and the fourth subfigure of Fig. 9 illustrates the positions that result in the desired outcome.

Figure 10 shows the trend of *p* during the iteration process of the multi-UAV formation, where the blue line represents the trend. The other four subplots in Fig. 9 depict the positions of UAVs in the system for different values of *p* as shown in Fig. 10. As the UAVs continue to move in the system, the overall system robustness also varies. As shown in Fig. 10, the value of *p* gradually approaches the target value of 7/12 starting from 0. By the 60th iteration, the system robustness has exceeded the target value. However, since the number of UAVs must be an integer, the robustness continues to converge even after reaching the target value, eventually reaching 1. However, this situation diminishes as the number of UAVs increases. In the fourth subfigure of Fig. 9, we also present the desired final position display in the subplot $p = 1$, which clearly shows that as the UAVs approach each other, the system's robustness increases.

In alignment with the previously elucidated strategy, Figs. 12 and 13 delineate the variation in inputs within a UAV swarm in response to the mobility of the formation. The observed similarity in input trends for both strategies can be attributed to their implementation via Eq. (7). As discussed in Sec. 3.2, concerning the function we constructed, it is noted that the control input consistently decreases as the inter-UAV distance reduces.

Presently, in accordance with the f_{attacker}-*fraction* local model outlined in [30], we define the system such that each
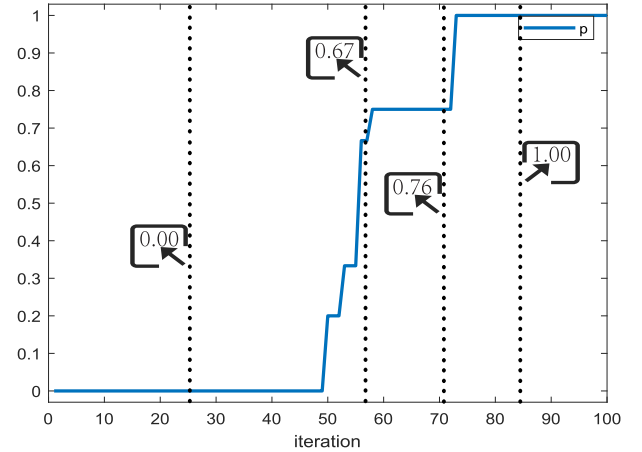

Fig. 10.   The trend graph for the values of *p* is represented. The four boxes correspond to the four positions in Fig. 9, each showing the values of *p*.
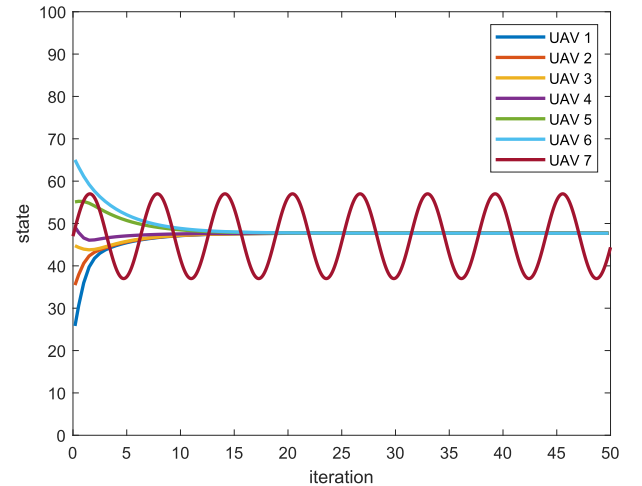

Fig. 11.   Consensus diagram depicts the scenario of UAV 7 as a malicious attacker, indicating that each UAV in the system can resist attackers with 1/6 the number of neighbors, that is, the other six UAVs can still achieve resilience despite being interfered with.
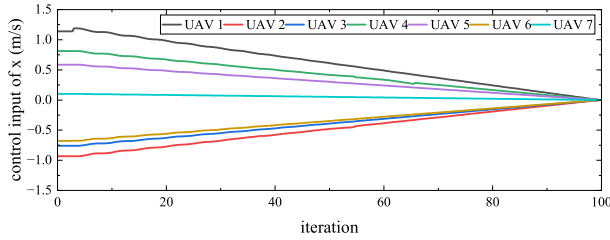
Fig. 12.   This graph shows the trend of changes for control input in x when the UAV cluster constructs a *p-fraction* robust formation.
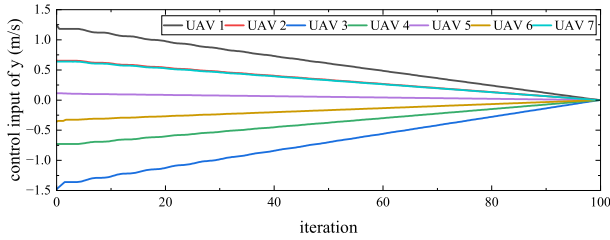

Fig. 13.   This graph shows the trend of changes for control input in y when the UAV cluster constructs a *p-fraction* robust formation.

node is capable of withstanding a proportion of malicious attackers equal to $f_{\mathrm{attacker}} = 1/6$ relative to the total number. Additionally, we ensure that $2f_{\mathrm{attacker}} = 1/3 < p \leq 1$, signifying the system's capacity to counteract the impact of one malicious attacker. As shown in Fig. 11, where UAV 7 is designated as the attacker, and the initial state of each UAV is set randomly, it is evident that ultimately, all nodes achieve resilient consensus. Obviously, the control strategy of *p-fraction* robust formation proposed in this paper is proved to be feasible with Figs. 10 and 11.

6.   Conclusion

In this paper, two novel robust formation control algorithms are designed for multi-UAV systems in the presence of malicious attacks. The first one employs the FCBF to construct a formation within a finite time, with its communication graph satisfying the (r, s)-robust properties. While the second algorithm utilizes the FCBF to build a *p-fraction* robust communication network. Both strategies transform a formation of randomly positioned UAVs on a plane into a communication graph that satisfies robust properties, thereby enhancing the robustness of the multi-UAV system against network attacks. Furthermore, simulations are conducted to validate the designed controllers. Future research directions include exploring time-varying, communication-delayed, or discontinuous communication topologies in multi-UAV formation problems, using

intelligent control methods, and establishing real platforms to validate the performance of the controllers.

ORCID

Zhaoming Zhang https://orcid.org/0009-0005-2962-6693
Yiming Wu https://orcid.org/0000-0001-9766-2307
Jie Jiang https://orcid.org/0009-0005-9252-9925
Ning Zheng https://orcid.org/0000-0003-3503-8167
Wei Meng https://orcid.org/0000-0002-8513-5013

References

[1]   L. A. V. Reyes and H. G. Tanner, Flocking, formation control, and path following for a group of mobile robots, *IEEE Trans. Control Syst. Technol.* **23**(4) (2014) 1268–1282.

[2]   S. Hayat, E. Yanmaz and R. Muzaffar, Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint, *IEEE Commun. Surv. Tutor.* **18**(4) (2016) 2624–2661.

[3]   C. B. Georgy Skorobogatov and E. Salami, Multiple UAV systems: A survey, *Unmanned Syst.* **8**(2) (2020) 149–169.

[4]   E. Garcia, D. W. Casbeer, Z. E. Fuchs and M. Pachter, Cooperative missile guidance for active defense of air vehicles, *IEEE Trans. Aerosp. Electron. Syst.* **54**(2) (2017) 706–721.

[5]   H. Yao, R. Qin and X. Chen, Unmanned aerial vehicle for remote sensing applications — a review, *Remote Sens.* **11**(12) (2019) 1443.

[6]   Q. Dong and C. Zhang, Trajectory optimization for RLV in TAEM phase using adaptive Gauss pseudospectral method, *Sci. China Inf. Sci.* **62**(1) (2019) 10206–1.

[7]   Y. Zhi, L. Liu, B. Guan, B. Wang, Z. Cheng and H. Fan, Distributed robust adaptive formation control of fixed-wing UAVs with unknown uncertainties and disturbances, *Aerosp. Sci. Technol.* **126** (2022) 107600.

[8]   M. Santilli, M. Franceschelli and A. Gasparri, Dynamic resilient containment control in multirobot systems, *IEEE Trans. Robot.* **38**(1) (2021) 57–70.

[9]   H. Li, Q. Liu, G. Feng and X. Zhang, Leader–follower consensus of nonlinear time-delay multiagent systems: A time-varying gain approach, *Automatica* **126** (2021) 109444.

[10]   W. Yao, B. Lin, B. D. Anderson and M. Cao, Guiding vector fields for following occluded paths, *IEEE Trans. Autom. Control* **67**(8) (2022) 4091–4106.

[11]   M. Z. Romdlony and B. Jayawardhana, Stabilization with guaranteed safety using control Lyapunov–barrier function, *Automatica* **66** (2016) 39–47.

[12] S. Ouahouah, M. Bagaa, J. Prados-Garzon and T. Taleb, Deep-reinforcement-learning-based collision avoidance in UAV environment, *IEEE Int. Things J.* **9**(6) (2021) 4015–4030.

[13] W. Yao, B. Lin and M. Cao, Integrated path following and collision avoidance using a composite vector field, in *IEEE 58th Conf. Decision and Control* (IEEE, 2019), pp. 250–255.

[14] A. Allam, A. Nemra and M. Tadjine, Parametric and implicit features-based UAV–UGVs time-varying formation tracking: Dynamic approach, *Unmanned Syst.* **10**(2) (2022) 109–128.

[15] C. Wei, X. Wu, B. Xiao, J. Wu and C. Zhang, Adaptive leader-following performance guaranteed formation control for multiple spacecraft with collision avoidance and connectivity assurance, *Aerosp. Sci. Technol.* **120** (2022) 107266.

[16] S. Shi, Z. Wang, Q. Song, M. Xiao and G.-P. Jiang, Leader-following quasi-bipartite synchronization of coupled heterogeneous harmonic oscillators via event-triggered control, *Appl. Math. Comput.* **427** (2022) 127172.

[17] I. Bayezit and B. Fidan, Distributed cohesive motion control of flight vehicle formations, *IEEE Trans. Indust. Electron.* **60**(12) (2012) 5763–5772.

[18] J. Li, B. Zhang, L. Cui and S. Chai, An extended virtual force-based approach to distributed self-deployment in mobile sensor networks, *Int. J. Distri. Sensor Netw.* **8**(3) (2012) 417307.

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

[20] A. D. Ames, X. Xu, J. W. Grizzle and P. Tabuada, Control barrier function based quadratic programs for safety critical systems, *IEEE Trans. Autom. Control* **62**(8) (2016) 3861–3876.

[21] A. Li, L. Wang, P. Pierpaoli and M. Egerstedt, Formally correct composition of coordinated behaviors using control barrier certificates, in *IEEE/RSJ Int. Conf. Intelligent Robots and Systems* (IEEE, 2018), pp. 3723–3729.

[22] K. Garg and D. Panagou, Robust control barrier and control Lyapunov functions with fixed-time convergence guarantees, in *American Control Conf.* (IEEE, 2021), pp. 2292–2297.

[23] L. Guerrero-Bonilla and V. Kumar, Realization of *r*-robust formations in the plane using control barrier functions, *IEEE Control Syst. Lett.* **4**(2) (2020) 343–348.

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

[25] D. Meng, Y. Jia, J. Du and J. Zhang, On iterative learning algorithms for the formation control of nonlinear multi-agent systems, *Automatica* **50**(1) (2014) 291–295.

[26] W. Chen, S. Hua and S. S. Ge, Consensus-based distributed cooperative learning control for a group of discrete-time nonlinear multi-agent systems using neural networks, *Automatica* **50**(9) (2014) 2254–2268.

[27] R. Yang, L. Liu and G. Feng, An overview of recent advances in distributed coordination of multi-agent systems, *Unmanned Syst.* **10**(3) (2022) 307–325.

[28] L. Guerrero-Bonilla, A. Prorok and V. Kumar, Formations for resilient robot teams, *IEEE Robot. Autom. Lett.* **2**(2) (2017) 841–848.

[29] H. Zhang and S. Sundaram, Robustness of information diffusion algorithms to locally bounded adversaries, in *American Control Conf.* (IEEE, 2012), pp. 5855–5861.

[30] H. J. LeBlanc, H. Zhang, X. Koutsoukos and S. Sundaram, Resilient asymptotic consensus in robust networks, *IEEE J. Select. Areas Commun.* **31**(4) (2013) 766–781.

[31] W. Ren and R. W. Beard, Consensus seeking in multiagent systems under dynamically changing interaction topologies, *IEEE Trans. Autom. Control* **50**(5) (2005) 655–661.

[32] W. Ren, R. W. Beard and E. M. Atkins, Information consensus in multivehicle cooperative control, *IEEE Control Syst. Mag.* **27**(2) (2007) 71–82.

Zhaoming Zhang received B. E. degree in network engineering from the Hangzhou Dianzi University, Hangzhou, China, in 2021. He is currently working toward his M.S. degree in cyberspace security with the School of Cyberspace, Hangzhou Dianzi University, Hangzhou, China. His current research interests include multi-agent systems and formation control.

Jie Jiang currently working toward the M.S. degree in cyberspace security with the School of Cyberspace, Hangzhou Dianzi University, Hangzhou, China. His main research interests include resilient consensus control, distributed optimization and distributed system security.

Yiming Wu received his B.Eng. degree in automation and the Ph.D. degree in Control Science and Engineering from the Zhejiang University of Technology, Hangzhou, China, in 2010 and 2016, respectively. He held visiting position from 2012 to 2014 with the School of Electrical and Electronic Engineering, the Nanyang Technological University, Singapore. Since July 2016, he has been at the Hangzhou Dianzi University, Hangzhou, China, where he is currently Associate Professor at the School of Cyberspace. His main research interests include multi-agent systems, security and privacy theory, iterative learning control, and applications in intelligent transportation systems and UAV swarm.

Ning Zheng received the M.S. degree in computer application from Zhejiang University, Hangzhou, China, in 1990. He is currently a Full Professor with the School of Cyberspace, Hangzhou Dianzi University, Hangzhou, China. His current research interests include multi-agent security, information management systems, and privacy preservation.

Wei Meng received the B.E. and M.E. degrees from Northeastern University, Shenyang, China, in 2006 and 2008, respectively, both in electrical engineering, and the Ph.D. degree in control and instrumentation from the Nanyang Technological University, Singapore, in 2013. From 2012 to 2017, he was a Research Scientist with UAV Research Group, Temasek Laboratories, National University of Singapore. He is currently with the School of Automation, Guangdong University of Technology as a Professor. His current research interests include unmanned systems, cooperative control, multirobot systems, localization, and tracking.