Swarm Robotic Flocking With Aggregation Ability Privacy

Shuai Zhang, Yunke Huang, Weizi Li, and Jia Pan, *Senior Member, IEEE*

***Abstract*— We address the challenge of achieving flocking behavior in swarm robotic systems without compromising the privacy of individual robots' aggregation capabilities. Traditional flocking algorithms are susceptible to privacy breaches, as adversaries can deduce the identity and aggregation abilities of robots by observing their movements. We introduce a novel control mechanism for privacy-preserving flocking, leveraging the Laplace mechanism within the framework of differential privacy. Our method mitigates privacy breaches by introducing a controlled level of noise, thus obscuring sensitive information. We explore the trade-off between privacy and utility by varying the differential privacy parameter ϵ. Our quantitative analysis reveals that $\epsilon \leq 0.13$ represents a lower threshold where private information is almost completely protected, whereas $\epsilon \geq 0.85$ marks an upper threshold where private information cannot be protected at all. Empirical results validate that our approach effectively maintains privacy of the robots' aggregation abilities throughout the flocking process.**

***Note to Practitioners*—This paper was motivated by the problem of preserving privacy of individual robots in a swarm robotic system. Existing approaches to address this issue generally consider that accomplishing complex tasks requiring explicit information sharing between robots, while explicit communication in public channel carries the risk of information leakage. It is not always like this in real adversarial environments, and this assumption restricts the investigation of privacy in autonomous systems. This paper suggests that an individual robot can use its sensors onboard to perceive states of other neighbors in a distributed way without explicit communication. Despite avoiding information leakage during explicit information sharing between robots, the configuration of swarm can still reveal sensitive information about the ability of each robot. In this paper, we propose a privacy-preserving approach for flocking control using the Laplace mechanism based on the concept of differential privacy. The solution prevents an adversary with full knowledge of the swarm's configuration from learning the sensitive information of individual robots, thus ensuring the security of swarm robots in terms of sensitive information during ongoing missions.**

Received 29 August 2024; revised 1 December 2024; accepted 31 December 2024. This article was recommended for publication by Associate Editor W. Wang and Editor P. Rocco upon evaluation of the reviewers' comments. This work was supported in part by The Government of the Hong Kong Special Administrative Region (HKSAR) Research Grants Council (RGC) General Research Fund (GRF) The University of Hong Kong (HKU) under Grant 11202119 and Grant 11207818 and in part by the Innovation and Technology Commission of HKSAR Government under InnoHK Initiative. *(Corresponding author: Jia Pan.)*

Shuai Zhang, Yunke Huang, and Jia Pan are with the Department of Computer Science and the TransGP Centre, The University of Hong Kong, Hong Kong (e-mail: shuaizhang2017@gmail.com; seahyk0909@gmail.com; jpan@cs.hku.hk).

Weizi Li is with the Min H. Kao Department of Electrical Engineering and Computer Science, The University of Tennessee at Knoxville, Knoxville, TN 37996 USA (e-mail: weizili@utk.edu).

Digital Object Identifier 10.1109/TASE.2025.3526141

***Index Terms*— Differential privacy, distributed robot systems, multi–robot systems, swarm robotics.**

I. Introduction

SIMULATING collective behaviors such as birds flocking and fish schooling have attracted great attention from the robotics community. These collective movements show that impressive global behaviors can emerge from limited local interactions between individuals and their environment [1], [2]. This recognition has inspired the development of decentralized swarm robotic systems to perform collective tasks that cannot be accomplished by a single robot or are performed more efficiently by a swarm robotic system [3], [4], [5], [6], [7], [8], [9], [10]. Despite the scalability, flexibility, and robustness provided by decentralization, privacy remains poorly addressed in swarm robotics. This is because individual robots in a swarm do not seem to be private entities who naturally wish to preserve the confidentiality of their data when performing collective tasks specified by a human designer.

Privacy is becoming an important issue in swarm robotic systems, especially in adversarial scenarios [11]. For example, a robot's motion can reveal sensitive information about its role within the group, allowing an adversary to recognize the leader and carry out an accurate attack [12]. Similar risks arise in tracking privacy or target privacy, where a swarm robotic system is expected to track a sequence of way-points or targets that are considered private information [13], [14], [15]. We underscore that security is an essential element of swarm control systems. It guarantees the privacy of control strategies and individual attributes, thereby preventing any adverse effects on the system's performance and upholding the integrity of the swarm's autonomous operations.

We endeavor to attain flocking behavior within a swarm robotic system, with a particular focus on preserving the privacy of each robot. We address the scenario wherein the protection of an individual robot's private information, specifically its aggregation ability, is paramount. The concept of aggregation ability encompasses constraints such as sensing range, minimum execution space, and safety clearance. The aggregation ability is selected to be privacy-sensitive due to its direct correlation with the strategic positioning and movement patterns of the robot swarm. The potential leakage of such private information could facilitate malicious interference, adversaries may exploit this vulnerability to devise targeted attack policies, thereby precipitating security breaches and potentially disastrous consequences. We are now facing a dilemma: on one hand, we need to generate the flocking behavior by using the database consisting of every robot's

private information (aggregation ability); on the other hand, we need to make sure that no adversary can infer the private information of any individual robot from the available configuration observed.

Our premise is that the configuration of swarm robots can reveal sensitive information about each robot's ability (e.g., aggregation abilities) even though the information leakage can be avoided if there is no explicit communication between robots, thus it is necessary to propose a privacy-preserving controller for swarm robotic flocking. This is a crisply formulated instance of the broader requirement of preserving privacy in swarm robotic applications: the robots can achieve complex tasks in a distributed fashion without explicit communication, thus avoiding information leakage during information sharing. However, the configurations of group, the behavioral difference between robots, as well as the specific moving patterns can also reveal sensitive information of individual robots in an implicit way. Our contributions are as follows.

- We emphasize that the configuration of swarm flocking can reveal the sensitive information about individual robots' aggregation abilities even though the information leakage caused by explicit communication between robots is avoided.
- We developed a differentially private mechanism that is independent from swarm size to protect the aggregation ability privacy of individual robots in swarm robotic flocking.
- We provided a theoretical analysis of how to set the sensitivity of Laplace mechanism with respect to the aggregation ability privacy.
- We found that an adversary's ability to infer the aggregation ability of a changing robot decreases as the value of the differential privacy parameter ϵ decreases. Specifically, $\epsilon \leq 0.13$ represents a lower bound where private information is almost completely protected, while $\epsilon \geq 0.85$ marks an upper threshold where private information cannot be protected at all.

The remainder of this paper is organized as follows. The related work is reviewed and compared to our work in Section II. In Section III the basic assumptions, the threat model of an adversary, the notation of differential privacy as well as the problem formulation are formalized in preliminaries. In Section IV we present the system model of swarm robotic flocking. In Section V, we propose the differentially private swarm robotic flocking algorithm. In Section VI, a series of numerical simulations are carried out to demonstrate the effectiveness of the proposed scheme, followed by a discussion on the general requirement of a privacy-preserving mechanism in swarm robotic systems. Finally, we conclude the paper in Section VIII.

II. Related Work

Huge amounts of data including image, video, audio, and text are ubiquitously generated every second, and it is becoming a great challenge to protect sensitive information when sharing them. In the last few years, the notion of *differential privacy* has emerged essentially as a standard privacy specification, which is originally proposed in [16]. It presents that a system is made *differentially private* by randomizing its answers in such a way that the published outputs are not too sensitive to the data provided by any single participant. It is proved that such differentially private scheme based on random mechanisms makes it difficult for an adversary to infer about individual records from the published outputs, or even to detect the presence of an individual in the database. As a result, sensitive information about individuals is differentially preserved. Differential privacy plays a key role in balancing the trade-off between data sharing and data privacy. It differs from our common understanding of privacy, here the privacy is measured on a level that changes continuously.

The concept of differential privacy has been widely used in industry [17], [18], [19]. For example, in privacy-aware traffic flow prediction, the traffic sensor data are usually stored by different organizations or parties, which implies impracticable data sharing due to concerns of privacy [20]. Data to be released to the public are also sensitive in large-scale medical databases due to confidentiality and privacy concerns [21]. The requirement to preserve privacy in government agencies is more serious than that in industry because government agencies typically need to take great potential risks of information leakage whenever they publish statistics based on their data collected from organizations, parties, and individuals [22]. Various differentially private mechanisms have been proposed to address these requirements. We refer interested readers to [23] for more details about the concept of differential privacy and its applications.

As large swarm robotic systems become more widespread, concerns are growing about the collection and use of sensitive data obtained from individual robots [24]. These issues are increasingly important in adversarial scenarios, where individual robots must share private information to achieve coordination and collective motion at the group level. However, information sharing carries the risk of information leakage, making privacy preservation in swarm robotics an inevitable issue. Although necessary, swarm robotic researchers rarely study it.

Several works have emerged using the concept of differential privacy in swarm robotics in recent years. In [25], the authors focused on the role privacy of heterogeneous robots in a swarm. They proposed a macroscopic privacy model based on differential privacy to keep information about individual robot types private and preserve security and resilience against adversaries. More recently, the work in [12] studied a specific leader-follower structure for private flocking control with swarm robots in terms of role privacy. They aimed to protect the leader's identity, which is considered sensitive information. The research on role privacy is designed to conceal the specific roles of individual robots within heterogeneous swarms from adversaries. Nonetheless, swarm robotic systems typically utilize homogeneous robots, which operate anonymously to execute tasks collectively. Consequently, in such scenarios, the concern for role privacy becomes redundant.

Another important area of study is tracking privacy and target privacy, where robots are controlled to track preference vectors or specific targets in a privacy-preserving manner. In [13], the authors considered a swarm system where each robot has a sequence of private way-points and a local controller designed to track them. They used the Laplace mechanism for data sharing, where each robot shares noisy versions of its state information with others, preventing any

TABLE I
A SUMMARY OF PRIVACY STUDY IN ROBOTIC SYSTEMS

Author (year)	Privacy	Objective	Subject	Inform. sharing	Application
Prorok et al. (2016)	Role privacy	Challenging adversaries in identifying individual robot types	Heterogeneous robot swarms	Yes	Collaborative task
Zheng et al. (2020)	Leader privacy	Obfuscating the flock leader from adversaries	Leader-follower framework	No	Private flocking
Wang et al. (2017)	Tracking privacy	Concealing tracking preferences from adversaries	Linear distributed systems	Yes	Collective motion
Chen et al. (2021)	Tracking privacy	Striking a balance between location privacy and semantic security	Vehicles	No	Vehicular network
Brodt and Pierson (2023)	Tracking privacy	Creating altered paths to conceal the goal from adversaries	Multi-robot systems	No	Multi-robot coverage
Zhang and Shell (2019)	Target privacy	Concealing the panda's location from adversaries	Robot	No	Protect the panda
Fiore and Russo (2019)	Consensus privacy	Securing consensus and non-faulty agents' data against adversaries	Multi-agent systems	Yes	Resilient consensus
Dong et al. (2021)	Consensus privacy	Ensuring agent cost function privacy throughout consensus	Multi-agent systems	Yes	Distributed control
Zhang et al. (2022)	Consensus privacy	Shielding private reference signals from adversaries	Multi-robot systems	Yes	Formation control
Nozari et al. (2016)	Optimization privacy	Minimizing objective sums while ensuring function privacy	Conv. const. optimization	Yes	Optimization problem
Lv et al. (2020)	Optimization privacy	Minimizing objective sums while ensuring function privacy	Multi-agent systems	Yes	Optimization problem
Zhang et al. (2024)	Optimization privacy	Obscuring solution positions in SI algorithms from adversaries	Swarm intelli. algorithms	Yes	Optimization problem
Ours (2024)	**Aggregation ability privacy**	**Obfuscating the robot's aggregation ability from adversaries**	**Homogeneous robot swarms**	**No**	**Private flocking**

robot from precisely estimating the aggregate state of the system. Although the performance of the swarm system was worse than that under perfect information sharing, tracking privacy was preserved. Similar attempts were reported in [14], which derived from the panda tracking problem. Here, the robot must maintain estimates of the panda's pose, but leaked information that is too precise poses an unexpected intrusion and hazard. A powerful adversary with access to the full history of information is interested in obtaining the panda's location. The problem here is the dilemma of tracking a target while preserving its position privacy. The work in [15] proposed a framework for generating privacy-aware trajectories in multi-robot coverage control applications, creating altered paths to conceal the goal of robots from adversaries. The authors in [26] developed an optimized differential privacy scheme with reinforcement learning to establish a balance between location privacy and semantic security. The research on tracking privacy and target privacy is designed to obfuscate the objectives of robots dependent on extrinsic assignments. However, the fundamental characteristics of robots cannot be concealed during the task.

The third area is the optimal consensus with respect to privacy, which has attracted the attention of robotic researchers [27], [28], [29], [30]. To achieve consensus, robots must exchange their state information with each other on a public channel. Adversaries can monitor the public channel and obtain the private information of individual robots, leading to a significant risk of information leakage. One study addressed this privacy requirement in the optimal consensus problem by using differential privacy and event-trigger schemes, preserving the privacy of the cost function of each robot during the consensus computation [29]. From the perspective of optimization [31], [32], existing swarm intelligence algorithms can be developed into the corresponding private versions by considering the concept of differential privacy. The investigation into such privacy preservation dilemmas relies on explicit information sharing, where the agents are required to reciprocate their state data or individual cost metrics mutually. While these solutions are efficacious in safeguarding the privacy of individual functions, it becomes untenable in scenarios prohibiting the exchange of information.

Our work differs from previous studies in several ways, as summarized in Table I. First, unlike [12], [25], we focus on swarms with homogeneous robots with strong anonymity, eliminating the need for role privacy. The swarm robotic flocking adopts a leaderless framework that generates flocking patterns rather than using a leader-follower scheme. Second, previous works [13], [14], [27], [28], [29], [30], [31], [32] relied on explicit information sharing and required robots to share noisy versions of their states using a randomized mechanism to achieve tracking privacy, target privacy, consensus and optimization. In contrast, our work aims to achieve privacy-preserving flocking behavior without explicit information sharing, as a focal robot can use its sensors onboard to perceive the states of other neighbors in a distributed way without explicit communication. Despite avoiding information leakage during explicit information sharing between robots, the swarm's configuration can still reveal sensitive information about each robot's ability. To this end, our focus is to propose a solution that can protect the swarm system from an adversary with full knowledge of the swarm's configuration to learn the sensitive information of individual robots.

III. PRELIMINARIES

In this section, we present the basic assumptions, the threat model of an adversary, the general notation of differential privacy, and then we formulate the problem.

A. Basic Assumptions

We consider swarm robotic flocking with cohesion preference, where individual robots generate flocking behavior by implicitly aggregating with others. The flocking configuration is influenced by each individual robot's aggregation ability. It is defined as follows.

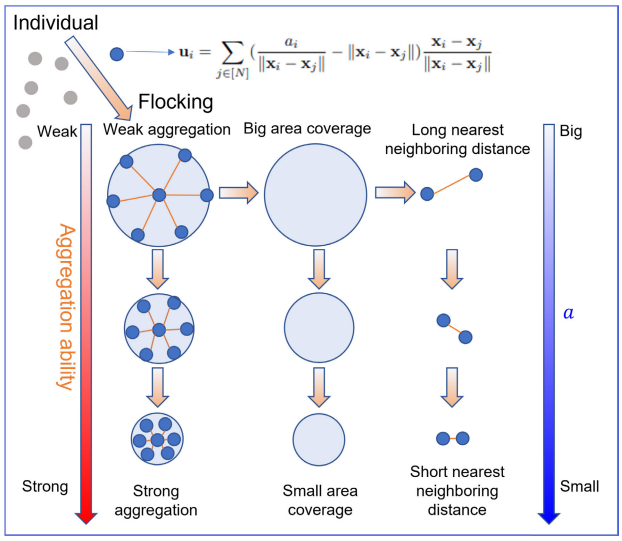


Fig. 1. Illustration of aggregation abilities of individual robots with respect to flocking pattern.

Definition 1 (Aggregation ability): The aggregation ability is an intrinsic property of a robot, influenced by constraints such as sensing range, minimum execution space, and safety clearance. This ability dictates the closest distance to neighboring robots in a flocking configuration and is considered confidential information for each robot.

As shown in Fig. 1, robots with strong aggregation abilities generate a compact configuration that has a small area coverage and a short nearest neighboring distance, while those with weaker aggregation abilities generate a looser configuration that has a greater area coverage and a longer nearest neighboring distance. We consider only the distance between robots as an indication of aggregation ability, because it can reveal aspects of the flocking strategy and adaptive behaviors that are proprietary to our control algorithm.

A swarm of n robots can generate a stable flocking pattern from an initial distribution with a limited time t_0 under the following assumptions:

- The aggregation ability is a robot's private information;
- The stable flocking configuration is solely determined by the aggregation abilities of all group members;
- There is no explicit information exchange between robots, the adversaries cannot collect confidential messages carrying aggregation ability information of individual robots;
- However, the adversaries can infer aggregation ability of individual robots after t_0 by observing the stable flocking configuration.

B. Threat Model

It is assumed that information leakage will not occur during information exchange since there is no information sharing between robots. However, an adversary can still infer private information of individual robots by observing the stable flocking configuration. In this work, we assume a highly-capable adversary, as described in [15], that

- possesses complete knowledge of the configuration of swarm robotic system;
- knows the global position of every robot in the flocking group;
- knows the aggregation model of flocking control but has no idea of each robot's control parameter.

To better demonstrate the performance of our approach, we assume that there is only one changing robot that has a different aggregation ability. The goal of the adversary is to infer

- Which robot has a different aggregation ability?
- What is the aggregation ability of this robot?

The adversary uses one known privacy attack policy as follows:

1) Changing Robot Inference: Since the adversary is aware of the global positions of all robots in the flocking group, it can thus determine the nearest neighboring distance of each individual robot based on this information. Let us denote the set of nearest neighboring distances as $D = \{d_i\}_{i=1}^n$, representing the adversary's observation. We can define the degree of deviation from the mean value to measure the discrepancy between the robot i and the other robots:

$$p_i = \frac{|d_i - \bar{d}|}{6\sigma}, \tag{1}$$

where $\bar{d}$ and σ are the mean and the standard deviation of observation D. A greater p_i suggests that the robot i is so different from other robots that it is more likely to be the changing robot. The robot with index c is then identified as the changing robot with respect to

$$c = \arg\max\{p_i\}, \quad i \in \{1, \cdots, n\}. \tag{2}$$

2) Aggregation Ability Inference: The aggregation ability of a robot can be approximately estimated by its nearest neighboring distance and the total number of group members. The adversary can approximately infer the aggregation ability of the changing robot by

$$a_c^* \approx \frac{n}{4} d_c^2, \tag{3}$$

where a_c^* characterizes the changing robot's aggregation ability and d_c is the nearest neighboring distance of the inferred changing robot. Please refer to Eq. (20) for more details of the derivation.

C. Differential Privacy

The notion of differential privacy has essentially emerged as a standard privacy specification [16]. It presents that a system is made differentially private by randomizing its answers in such a way that the published outputs are not too sensitive to the data provided by any single participant. To apply the concept of differential privacy into the swarm robotic flocking system, we provide some basic definitions and theorems about differential privacy as follows:

Definition 2 (Aggregation ability database): A set $A = \{a_i\}_{i=1}^n$, where a_i determines the aggregation ability of the robot i, is defined as the database that contains the information of aggregation abilities of swarm robots.

Definition 3 (Adjacent databases [33]): Two databases $A = \{a_i\}_{i=1}^n$ and $A' = \{a_i'\}_{i=1}^n$ are said to be adjacent if and only if there exists one different element between the two databases, i.e., there exists $k \in \{1, \cdots, n\}$ such that $a_k \neq a_k'$ and $a_i = a_i'$ for all $i \neq k$.

In the framework of differential privacy, the output to be released to the public that we compute from a database is modelled by $q(A)$ for some mapping q that acts on A. A mechanism approximating q that acts on a database is said to be differentially private if it guarantees that two adjacent databases are almost indistinguishable from the observation of the output. Concretely,

Definition 4 (ϵ-Differential privacy [16]): Given $\epsilon \geq 0$, a mechanism M preserves ϵ-differential privacy if for all $\mathcal{R} \subseteq \text{range}(M)$ and all adjacent databases A and A', it holds that

$$Pr[M(A) \in \mathcal{R}] \leq e^{\epsilon} \cdot Pr[M(A') \in \mathcal{R}]. \tag{4}$$

where $\epsilon \geq 0$ controls the privacy level, and $\epsilon = 0$ means perfect privacy while $\epsilon \to \infty$ refers to non-privacy. $\mathcal{R}$ denotes the set of all possible outputs, and $Pr[\cdot]$ measures the probability of outputs.

For two adjacent databases A and A' with respect to aggregation abilities of robots, the sensitivity, a concept that can describe the maximal difference of a function applied to the adjacent database, is defined as follows.

Definition 5 (Sensitivity [16]): The sensitivity of a differentially private mechanism M about aggregation ability in the flocking system is

$$\Delta u(t) = \max_{A,A'} \|M(A,t) - M(A',t)\|_1, \tag{5}$$

where Δu is the sensitivity in terms of control input under the control mechanism M. $\|x\|_1 = \sum_{i=1}^{|x|} |x_i|$ is the l_1 norm of a database x. $\|x - y\|_1$ is the l_1 distance between two databases x and y, and for the two adjacent databases A and A', we have $\|A - A'\|_1 = |a_k - a_k'|$ with $a_k \neq a_k'$ and $k \in \{1, \cdots, n\}$.

Proposition 1: The sensitivity of a differentially private mechanism M about aggregation ability in terms of velocity and position are:

$$\begin{aligned} \Delta v(t) &= \Delta u(t) \cdot dt, \\ \Delta x(t) &= \Delta v(t) \cdot dt = \Delta u(t) \cdot (dt)^2, \end{aligned} \tag{6}$$

where dt is the time interval in the discrete system model.

Proof: See Appendix. ■

D. Problem Formulation

Let $a_i \in A$ represent the aggregation ability of the robot i, then the problem of preserving aggregation ability privacy in swarm robotic flocking in terms of ϵ-differential privacy can be defined as:

Problem: Given $\epsilon \geq 0$, design a mechanism M for the flocking controller that is able to ensure

$$Pr[M(A) \in \mathcal{R}] \leq e^{\epsilon} \cdot Pr[M(A') \in \mathcal{R}] \tag{7}$$

for all $\mathcal{R} \subseteq \text{range}(M)$ and all adjacent databases A and A'. Here $M(A) = \{\mathbf{u}_i^{[M]}(a_i)\}_{i=1}^n$ is the set of improved controllers for all robots that lead to the stable flocking configuration under the database A. In other words, the proposed scheme needs to ensure that the probability of detecting a small change in the aggregation ability of one robot from observation should be very low.

IV. System Model

This work models a flocking system in $\mathbb{R}^2$ using the following integro-differential aggregation equation:

$$\begin{aligned} &\rho_t + \nabla \cdot (\rho v) = 0, \\ &v = -\nabla K * \rho, \end{aligned} \tag{8}$$

where ∇ means gradient, ρ represents aggregation density, K denotes inter-agent interaction potential and $*$ denotes convolution. The aggregation model can be rewritten as an agent-based model with pairwise interaction among n agents in $\mathbb{R}^2$:

$$\dot{\mathbf{x}}_i = -\sum_{j \in [N]} \nabla_i K(\mathbf{x}_i - \mathbf{x}_j), \quad i = 1, \cdots, n, \tag{9}$$

where $\mathbf{x}_i(t)$ is the position of the agent i at time t, and $[N]$ denotes the set of interaction neighbors within a limited sensing range δ_s. The sensing coverage area for each individual robot is defined by the range and field of view of the on-board sensors. We model this as a circular area centered on the robot, with a radius determined by the maximum effective range of the sensors. This equation can be used to model aggregations in swarm robotics that behave like flocking systems, such as bird flocks, fish schools, and bacterial colonies. We can extend this aggregation model to the double integrator system

$$\begin{aligned} \dot{\mathbf{x}}_i &= \mathbf{v}_i, \\ \dot{\mathbf{v}}_i &= \mathbf{u}_i, \\ \mathbf{u}_i &= -\sum_{j \in [N]} \nabla_i K(\mathbf{x}_i - \mathbf{x}_j) - \nabla_i U^{\text{vis}}, i = 1, \cdots, n. \end{aligned} \tag{10}$$

Here, in addition to the interaction between robots, a viscous potential $U^{\text{vis}} = \frac{1}{2}\xi \mathbf{v}_i^T \mathbf{v}_i$ is introduced to stabilize the second-order system. The viscous force is described by a damping term proportional to speed $-\nabla_i U^{\text{vis}} = -\xi \mathbf{v}_i$. The viscous force has no effect on the robots' stable configuration.

Aggregation in a flocking system is mainly determined by the interaction potential function K. In this study, the function in Eq. (11) is utilized to obtain a flocking system [34]:

$$K(x) = -a \ln \|\mathbf{x}\| + \frac{1}{2}\|\mathbf{x}\|^2, \tag{11}$$

where $\|\mathbf{x}\|$ represents the relative distance between two robots, and interactions depend only on this distance rather than actual robot locations. The robots' flocking behavior can be described by the interaction potential and the viscous potential as follows:

$$\begin{aligned} \dot{\mathbf{x}}_i &= \mathbf{v}_i, \\ \dot{\mathbf{v}}_i &= \mathbf{u}_i, i = 1, \cdots, n, \\ \mathbf{u}_i &= \sum_{j \in [N]} \left(\frac{a_i}{\|\mathbf{x}_i - \mathbf{x}_j\|} - \|\mathbf{x}_i - \mathbf{x}_j\|\right) \frac{\mathbf{x}_i - \mathbf{x}_j}{\|\mathbf{x}_i - \mathbf{x}_j\|} - \xi \mathbf{v}_i, \end{aligned} \tag{12}$$

where $a_i > 0$ is a parameter in each robot's local controller that determines the aggregation ability of the robot i.

V. Differentially Private Algorithm

Under the stable configuration, the parameter a_i in the dynamics Eq. (12) determines the radius of flocking system and the distance between adjacent robots given total number of robots. Thus, it characterizes the ability of each robot to

aggregate to generate the flock pattern. If an adversary can observe the configuration of the flocking system, they may accurately infer the aggregation ability of an individual robot by observing the distance between adjacent robots. To this end, our goal is to design a differentially private mechanism for the flocking controller that hides the aggregation ability of individual robots.

A. Privacy-Preserving Flocking Control

We are proposing a differentially private mechanism for the flocking system using the Laplace mechanism. The Laplace mechanism is one commonly used differentially private mechanism. It works by introducing additive noise into the query q that has the Laplace distribution.

Theorem 1: For the flocking system given by Eq. (12), let Δu be the sensitivity of mechanism M, then the mechanism $M = \{\mathbf{u}_i + w\}_{i=1}^n$ with $w \sim \text{Lap}(\Delta u/\epsilon, n)$ preserves ϵ-differential privacy.

Here $\text{Lap}(\lambda, n)$ means a n-dimensional random vector x obeys the laplace distribution with parameter λ (and zero mean), and its probability distribution function satisfies

$$p(x) = (\frac{1}{2\lambda})^n \exp(-\frac{\|x\|_1}{\lambda}). \tag{13}$$

Proof: Given $a_i \in A$, the control input $\mathbf{u}_i$ in Eq. (12) can be rewritten as

$$\begin{aligned}
\mathbf{u}_i(a_i, t) &= \mathbf{f}_i(a_i, t) + \mathbf{f}_i(t),\\
\mathbf{f}_i(a_i, t) &= \sum_{j\in[N]} a_i \left(\frac{\mathbf{x}_i(t) - \mathbf{x}_j(t)}{\|\mathbf{x}_i(t) - \mathbf{x}_j(t)\|^2}\right),\\
\mathbf{f}_i(t) &= -\sum_{j\in[N]} \big(\mathbf{x}_i(t) - \mathbf{x}_j(t)\big) - \xi \mathbf{v}_i(t).
\end{aligned} \tag{14}$$

For two adjacent databases $A = \{a_i\}_{i=1}^n$ and $A' = \{a_i'\}_{i=1}^n$ with $a_k \neq a_k'$ and $a_i = a_i'$ for all $i \neq k$, according to Eq. (5), the sensitivity of the mechanism M can be derived as

$$\begin{aligned}
\Delta u(t) &= \max_{A,A'} \|M(A, t) - M(A', t)\|_1\\
&= \max_{i\in\{1,\cdots,n\}} \sum_{i=1}^n |\mathbf{u}_i(a_i, t) - \mathbf{u}_i(a_i', t)|\\
&= \max_{k\in\{1,\cdots,n\}} |\mathbf{u}_k(a_k, t) - \mathbf{u}_k(a_k', t)|\\
&= \max_{k\in\{1,\cdots,n\}} |\mathbf{f}_k(a_k, t) + \mathbf{f}_k(t) - \mathbf{f}_k(a_k', t) - \mathbf{f}_k(t)|\\
&= \max_{k\in\{1,\cdots,n\}} |\mathbf{f}_k(a_k, t) - \mathbf{f}_k(a_k', t)|.
\end{aligned} \tag{15}$$

Let p_a and $p_{a'}$ denote the probability density function of $M(A, \mathbf{u}, \epsilon)$ and $M(A', \mathbf{u}, \epsilon)$ respectively. Compare the two at some arbitrary point $\mathbf{z} \in \mathbb{R}^2$

$$\begin{aligned}
&\frac{p_a(\mathbf{z})}{p_{a'}(\mathbf{z})}\\
&= \prod_{i=1}^n \left(\frac{\exp(\frac{-\epsilon|\mathbf{f}_i(a_i,t)+\mathbf{f}_i(t)-\mathbf{z}_i|}{\Delta u(t)})}{\exp(\frac{-\epsilon|\mathbf{f}_i(a_i',t)+\mathbf{f}_i(t)-\mathbf{z}_i|}{\Delta u(t)})}\right)\\
&= \prod_{i=1}^n \exp\left(\frac{\epsilon(|\mathbf{f}_i(a_i', t) + \mathbf{f}_i(t) - \mathbf{z}_i| - |\mathbf{f}_i(a_i, t) + \mathbf{f}_i(t) - \mathbf{z}_i|)}{\Delta u(t)}\right)\\
&\leq \prod_{i=1}^n \exp\left(\frac{\epsilon|\mathbf{f}_i(a_i, t) - \mathbf{f}_i(a_i', t)|}{\Delta u(t)}\right)\\
&= \exp\left(\frac{\epsilon\|\mathbf{f}(A, t) - \mathbf{f}(A', t)\|_1}{\Delta u(t)}\right)\\
&= \exp\left(\frac{\epsilon|\mathbf{f}_k(a_k, t) - \mathbf{f}_k(a_k', t)|}{\Delta u(t)}\right),
\end{aligned} \tag{16}$$

where the inequality follows from the triangle inequality as reported in [35]. According to Eq. (15), we have

$$\begin{aligned}
&\Delta u(t) \geq |\mathbf{f}_k(a_k, t) - \mathbf{f}_k(a_k', t)|\\
&\Rightarrow \exp\left(\frac{\epsilon|\mathbf{f}_k(a_k, t) - \mathbf{f}_k(a_k', t)|}{\Delta u(t)}\right) \leq \exp(\epsilon).
\end{aligned} \tag{17}$$

We then have

$$\frac{p_a(\mathbf{z})}{p_{a'}(\mathbf{z})} \leq \exp\left(\frac{\epsilon|\mathbf{f}_k(a_k, t) - \mathbf{f}_k(a_k', t)|}{\Delta u(t)}\right) \leq \exp(\epsilon). \tag{18}$$

Thus, the mechanism preserves ϵ-differential privacy with respect to aggregation ability. ■

Remark 1: According to Eq. (6), the sensitivity in terms of $\mathbf{u}$ can be equivalently expressed by $\mathbf{v}$ and $\mathbf{x}$, therefore, Theorem 1 holds when $\mathbf{u}$ is also replaced by $\mathbf{v}$ or $\mathbf{x}$.

B. Sensitivity in Flocking System

In this work, it is assumed that a swarm of robots can generate a stable flocking pattern from an initial distribution with a limited time t_0. The aggregation ability cannot be accurately inferred in unstable states during $0 < t < t_0$. To this end, the sensitivity under stable state (flocking pattern) is derived.

Theorem 2: For the flocking system with Eq. (12), given the adjacency relation by $|d_i - d_i'| \leq r_1 - r_0$, where $\{(r_0, r_1) : 0 < r_0 < r_1\}$ are the minimum and maximum nearest neighbor distance a robot can maintain, d_i and d_i' are the nearest neighboring distance of the robot i under the two adjacent databases A and A', respectively; then the sensitivity of the Laplace mechanism M is $\Delta u = \frac{n(r_1^2 - r_0^2)}{4r_0}$.

Proof: Without loss of generality, we assume that one of two adjacent aggregation ability databases has the same value for all its components, while allowing only one different component for its adjacent database. Specifically, we have $A = \{a, \cdots, a, a\}^n$ and $A' = \{a, \cdots, a, a'\}^n$ with $a \neq a'$. In such case, the robots aggregate and form a uniformly distributed flocking system, converging into a stable configuration with the following three properties, as proven in [34]:

1) The density ρ is uniform within a disk and zero outside;
2) For any robot position $\mathbf{x}_i(t)$ and given the swarm center $\mathbf{c}(t)$, there exists t_0 such that $\|\mathbf{x}_i(t) - \mathbf{c}(t)\| \leq R$ holds for all $t \geq t_0$, where R is less than the upper bound radius of the disk, $R_{\text{up}} = \sqrt{a}$;
3) Increasing the number of robots does not affect the radius or shape of the flock.

The distance between two adjacent robots is solely determined by the aggregation abilities of the robots given the group size of a flock. From this point, the *equivalent area principle* is used to calculate the relation between the nearest neighboring distance and the aggregation ability. At the stable state, given the radius R of the distribution disk, the number of robots n, and the nearest neighboring distance d (it is nearly the same for all robots in a uniformly distributed flock), there exists an

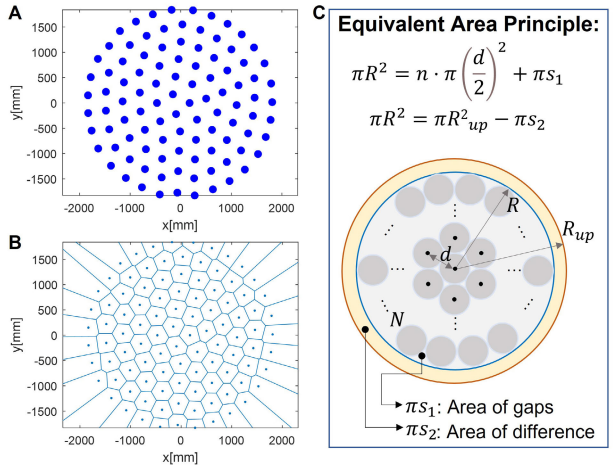


Fig. 2. The equivalent area principle for obtaining the relation between the private space d and the parameter a. (A) Under the ideal condition, the flock with Eq. (12) will spread into a loose pattern via a hexagonal close packing. (B) The Voronoi diagram of the flocking system. (C) The equivalent area principle derived from the hexagonal close packing. $n = 100$, $a = 2000^2$.

equivalent area description as follows:

$$\pi R^2 = n \cdot \pi (\frac{d}{2})^2 + \pi s_1$$
$$\pi R^2 = \pi R^2_{\text{up}} - \pi s_2. \tag{19}$$

As shown in Fig. 2(A-B), the flocking system with Eq. (12) will spread into a loose pattern via a hexagonal close pack. The pattern shows that each robot has a similar nearest neighboring distance d as the density is uniform inside the disk. The diagram in Fig. 2 (C) presents the equivalent area principle. Here πs_1 denotes the area of gaps among n flocking robots inside the disk with radius of R. πs_2 denotes the area of difference caused by the real radius R and the upper bound R_{up}. Substituting $R_{\text{up}} = \sqrt{a}$ to Eq. (19) yields

$$a = n\frac{d^2}{4} + s_1 + s_2. \tag{20}$$

For an adjacent database A', only one robot has a different aggregation ability in the flock, which means s_1 and s_2 could be considered unchanged. Therefore, we also have

$$a' = n\frac{d'^2}{4} + s_1 + s_2 \tag{21}$$

Now we can derive the sensitivity under the stable state as:

$$\begin{aligned}
\Delta u &= \max_{A,A'} \|M(A,t) - M(A',t)\|_1 \\
&= \max_{i\in\{1,\cdots,n\}} \sum_{i=1}^{n} \left|\mathbf{u}_i(a_i,t) - \mathbf{u}_i(a_i',t)\right| \\
&= \max_{i\in\{1,\cdots,n\}} \sum_{i=1}^{n} \left|\mathbf{f}_i(a_i,t) - \mathbf{f}_i(a_i',t)\right| \\
&= \max_{i\in\{1,\cdots,n\}} \sum_{i=1}^{n} \sum_{j\in[N]} \left| \frac{a_i}{\|\mathbf{x}_i(t) - \mathbf{x}_j(t)\|} - \frac{a_i'}{\|\mathbf{x}_i(t) - \mathbf{x}_j(t)\|} \right| \\
&= \max_{i\in\{1,\cdots,n\}} \left| \frac{a - a'}{\|\mathbf{x}_i(t) - \mathbf{x}_j(t)\|} \right| \\
&= \max_{i\in\{1,\cdots,n\}} \left| \frac{n(d^2 - d'^2)}{4\|\mathbf{x}_i(t) - \mathbf{x}_j(t)\|} \right| \\
&= \max_{i\in\{1,\cdots,n\}} \frac{n(r_1^2 - r_0^2)}{4\|\mathbf{x}_i(t) - \mathbf{x}_j(t)\|} \\
&= \frac{n(r_1^2 - r_0^2)}{4r_0}
\end{aligned} \tag{22}$$

■

The sensitivity based on the Laplace mechanism, captures the magnitude by which a single robot can change the stable configuration in the worst case. Intuitively, the uncertainty introduced into the flocking controller hides the aggregation ability of a single robot. Theorem 2 presents that how much we must perturb the outcome of proposed mechanism to preserve an individual robot's aggregation ability privacy characterised by nearest neighboring distance $|d_i - d_i'| \leq r_1 - r_0$. It also theoretically demonstrates that our proposed mechanism is effective in preserving aggregation ability privacy of swarm robotic flocking, i.e., despite the observation of a stable flocking configuration, an adversary cannot determine the nearest neighboring distance (aggregation ability) of any robot exactly except that it lies within $[r_0, r_1]$.

C. Measuring the Level of Aggregation Ability Privacy

Differential privacy differs from the common understanding of privacy, since it measures the level of privacy that changes continuously from perfect privacy to non-privacy. Taking inspiration from [13], we define a cost function to evaluate the level of aggregation ability privacy in the flocking system. The basic idea is that the difference between one robot's neighboring distance and that of the other robots implies the robot's aggregation ability and could be a clue for an adversary making inferences. Therefore, the difference between the nearest neighboring distance of an individual robot and the mean value of the robot group using the square error is used as the cost function.

The cost function for the robot i under the differentially private mechanism M is:

$$\text{cost}_i^{[M]}(t) = \mathbb{E}\Big[\big(d_i(t) - \bar{d}(t)\big)^2\Big], \tag{23}$$

where $d_i(t)$ is the nearest neighboring distance of the robot i at time t, $\bar{d}(t)$ is the mean value of all $d_i(t)$, and $\mathbb{E}$ denotes mathematical expectation.

The cost function under the original control policy (non-private mechanism) $\mathbf{u}$ is:

$$\text{cost}_i^{[u]}(t) = \big(d_i(t) - \bar{d}(t)\big)^2. \tag{24}$$

Level of aggregation ability privacy by mechanism M is defined as the supremum in the change of one robot's cost over all databases relative to the non-private mechanism:

$$P_{\text{space}} = \max_{i\in\{1,\cdots,n\}} \Big(\text{cost}_i^{[M]}(t) - \text{cost}_i^{[u]}(t)\Big). \tag{25}$$

In practice, a swarm robotic system can converge to the flocking pattern in a very short time, thus our approach can make a critical difference in preserving privacy of swarm robotics in flocking behavior, with a limited time not an infinite time. Generally, a higher P_{space} indicates better privacy, but this value will decrease as the system approaches a steady state over time.

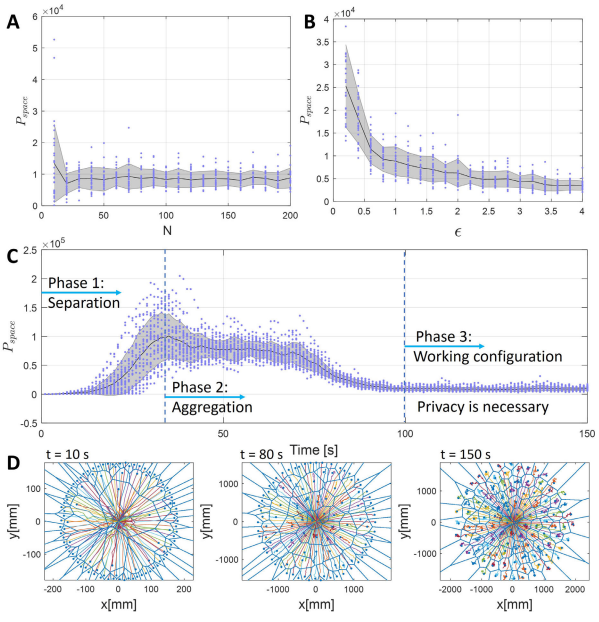


Fig. 3. The level of aggregation ability privacy for different number of robots n, differential privacy parameter ϵ and time horizon T. (A) The level of privacy versus n ($\epsilon = 1$). (B) The level of privacy versus ϵ ($n = 100$). (C) The level of privacy versus T ($n = 100$, $\epsilon = 1$). (D) The snapshots and trajectories of robots in three phases ($n = 100$, $\epsilon = 1$).

VI. Results and Discussion

Consider a swarm system in which each robot is a mass point on 2D plane moving with Eq. (12). Unless otherwise stated, the robots have $v_{\max} = 20$ mm/s, $u_{\max} = 100$ mm/s^2, $\zeta = 0.2$, $r_0 = 200$ mm, $r_1 = 400$ mm, and a limited sensing range $\delta_s = 1000$ mm. To better demonstrate the performance of our approach, we assume that there is only one robot that has a different aggregation ability while the others are characterized by the same value $a = 2000^2$. The objective of the adversary is to accurately infer which one is the changing robot and what its aggregation ability is as much as possible. On the other hand, the goal of the privacy-preserving mechanism is to hide the changing robot and to prevent the adversary from accurately inferring the aggregation ability of the changing robot.

A. Level of Aggregation Ability Privacy

We first study the level of aggregation ability privacy with simulation-based analysis. Each simulation is implemented 30 independent runs, and we record the level of aggregation ability privacy for different number of robots n, differential privacy parameter ϵ and time horizon T. The statistical results are shown in Fig. 3.

From Fig. 3A, as n increases from 20 to 200, the level of aggregation ability privacy is nearly unchanged. It means the level of privacy is independent of number of robots, demonstrating that the proposed privacy-preserving flocking controller with respect to aggregation ability privacy is scalable to the swarm size. The level of aggregation ability privacy and its variance increase with the decrease of the differential privacy parameter ϵ, as shown in Fig. 3B. This demonstrates that more privacy is preserved when ϵ becomes smaller. Fig. 3C shows the level of aggregation ability privacy versus time horizon, where the robots are initially deployed as a tight cluster. The flocking process can be characterized by three phases: separation, aggregation, and flocking, as shown in Fig. 3D. Repulsive force and attractive force dominate the separation phase and the aggregation phase, resulting in the dispersion and the aggregation of robots, respectively. Note that, under the phases of separation and aggregation, robots are in situations prior to the flocking configuration. The level of privacy is relatively higher and the aggregation ability cannot be accurately inferred at these unstable states. However, there is a significant decrease of privacy when robots get close to the flocking configuration (i.e., a relatively uniform distribution of robots as shown by Voronoi diagram in Fig. 3D, $t = 150$ s). This implies that an adversary may accurately infer the aggregation abilities of robots when they are in a flocking configuration, necessitating a safe controller to preserve aggregation ability privacy.

B. Comparison Results

Using the threat model described in Eq. (1)-(3), we evaluate the performance of differentially private mechanism in terms of preserving aggregation ability privacy during swarm robotic flocking. According to the concept of differential privacy, this can be done by evaluating the probability that a small change in the aggregation ability of one robot is detected from the observation. The baseline is given by changing one robot's aggregation ability and see the inference results without the differentially private mechanism.

As shown in Fig. 4A, a swarm robotic system without differentially private mechanism is in its flocking configuration with $a_c = 2100^2$ for the changing robot and $a = 2000^2$ for the other robots. The nearest neighboring distance of this changing robot can be easily identified according to the observation D (see threat model in preliminaries), as shown by the red line in Fig. 4(a2). The adversary can obtain every robot's degree of deviation with this observation, and the result shows that the greatest degree of deviation ($p_c = 0.94$) exactly points to the changing robot (denoted by the red line), indicating the adversary can accurately infer which one is the changing robot. Note that despite the aggregation ability is determined by a, the value of $\sqrt{a}$ has a more straightforward physical meaning about aggregation ability (i.e., the maximum area robots can aggregate). Compared to $\sqrt{a_c} = 2000$, the inferred value $\sqrt{a_c^*} = 2132$ is close enough, thus the adversary can also accurately infer the aggregation ability of this changing robot. Similar results can be obtained when the parameter of aggregation ability of the changing robot is decreased to $a_c = 1900^2$, as shown in Fig. 4B. The result shows that the greatest degree of deviation ($p_c = 0.92$) exactly points to the changing robot (denoted by the red line), indicating the adversary can again accurately infer which one is the changing robot. Furthermore, the adversary also has a relatively accurate inference about the aggregation ability of changing robot, $\sqrt{a_c^*} = 1949$ is close to $\sqrt{a_c} = 1900$.

The results with differentially private mechanism are shown in Fig. 5. From Fig. 5A-C, it is see that when $a_c = 2100^2$, the inference results depend on the parameter ϵ. When $\epsilon = 10$ or above, the swarm robotic system is totally incapable of hiding the changing robot and its aggregation ability: (1) the adversary can accurately infer which one is the changing robot because the changing robot exactly has the greatest degree

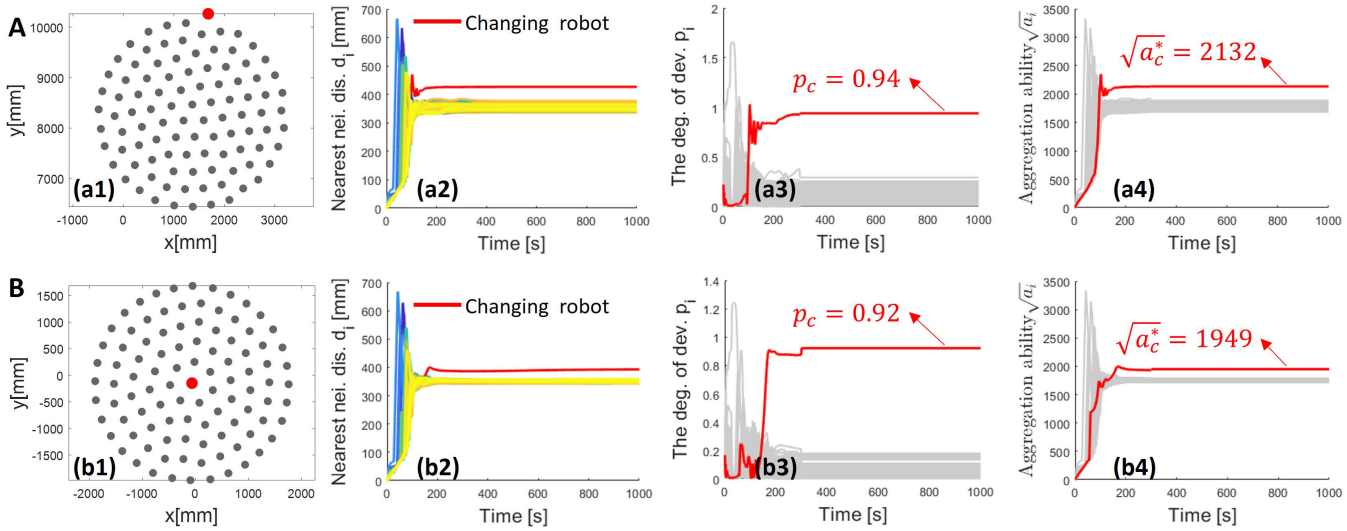


Fig. 4. The results of swarm robotic flocking without the privacy-preserving mechanism. (A) The flocking configuration and the inference results with $a_c = 2100^2$ for the changing robot and $a = 2000^2$ for the other robots. (B) The flocking configuration and the inference results with $a_c = 1900^2$ for the changing robot and $a = 2000^2$ for the other robots. $n = 100$ for both cases. Illustrative videos can be found in the supplementary material.

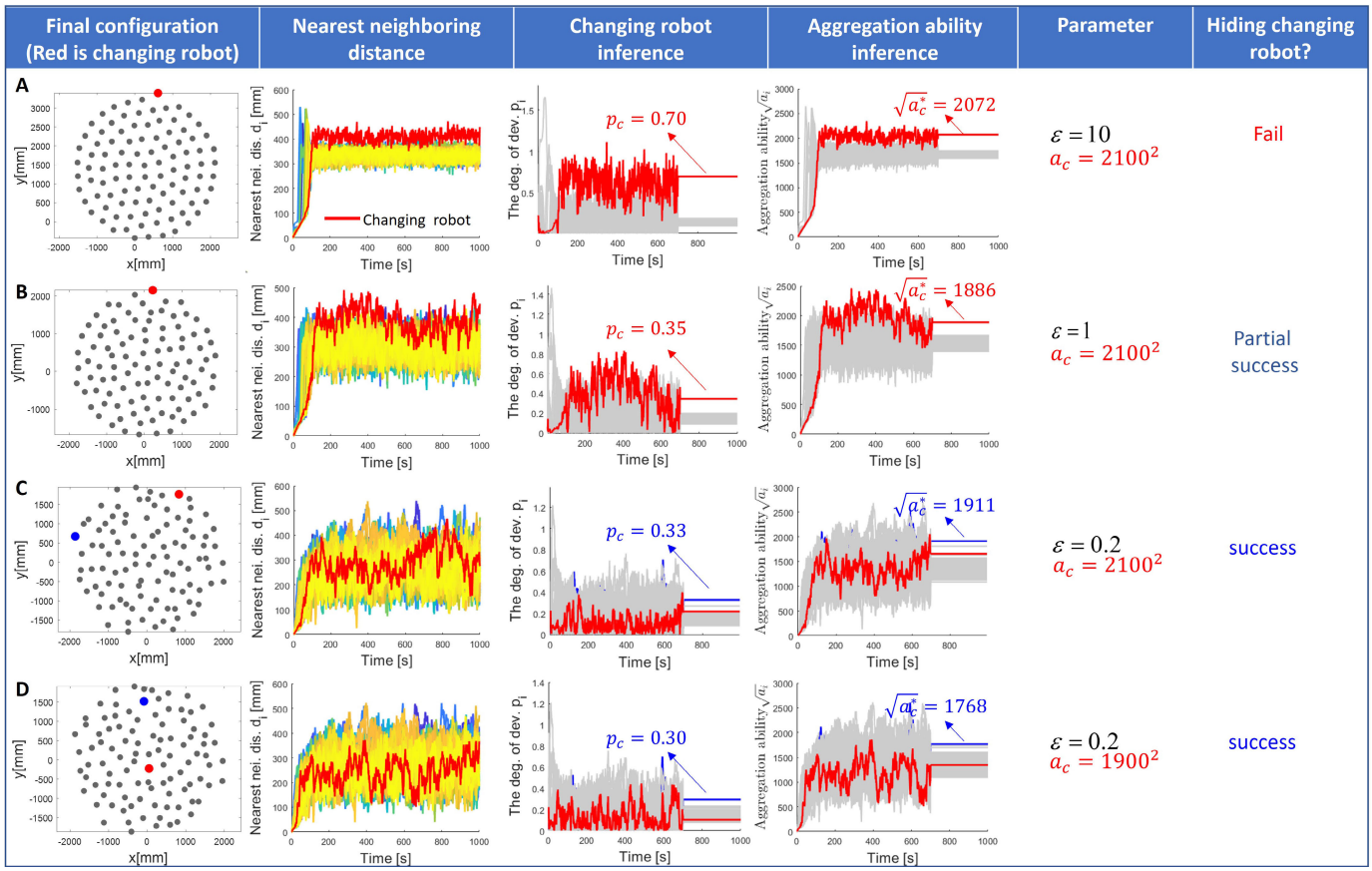


Fig. 5. The results of swarm robotic flocking with the privacy-preserving mechanism. The flocking configuration and the inference results with (A) $\epsilon = 10$ (B) $\epsilon = 1$ (C) $\epsilon = 0.2$, $a_c = 2100^2$ for the changing robot and $a = 2000^2$ for the other robots. (D) The flocking configuration and the inference results with $\epsilon = 0.2$, $a_c = 1900^2$ for the changing robot and $a = 2000^2$ for the other robots. $n = 100$ for all cases. Illustrative videos can be found in the supplementary material.

of deviation ($p_c = 0.70$), and (2) the inferred aggregation ability $\sqrt{a_c^*} = 2072$ is close to $\sqrt{a_c} = 2100$. If decrease the parameter to $\epsilon = 1$, the swarm robotic system can partially hide the changing robot and its aggregation ability: (1) the adversary can only accurately infer which one is the changing robot because the greatest degree of deviation $p_c = 0.35$ points to the changing robot, (2) however, it cannot accurately infer the changing robot's aggregation ability because the inferred $\sqrt{a_c^*} = 1886$ is far away from the practical $\sqrt{a_c} = 2100$. The swarm robotic system is totally capable of hiding the changing robot and its aggregation ability when the parameter is decreased to $\epsilon = 0.2$ or lower. In such case,

the adversary can neither correctly find the changing robot, nor its corresponding aggregation ability, because (1) the greatest degree of deviation ($p_c = 0.33$) points to one of normal robots (denoted by the blue line and the blue point) and (2) the aggregation ability of the changing robot is mistakenly inferred via this normal robot. A similar conclusion can be obtained when the aggregation ability parameter of the changing robot is decreased to $a_c = 1900$. For example, when $\epsilon = 0.2$, the swarm robotic system is totally capable of hiding the changing robot and its aggregation ability because it makes the adversary mistakenly identify the changing robot (the greatest degree of deviation ($p_c = 0.30$) points to one of normal robots denoted by the blue line and the blue point) and its corresponding aggregation level. In other words, the influence of parameter ϵ on the inference results demonstrates that the proposed scheme can continuously protect the level of aggregation ability privacy.

C. Effect of ϵ on Inference Results

We further evaluate the dynamic changes in the rate of discovery of private information caused by successive changes in ϵ. The quantitative correlation between inference results and ϵ is demonstrated by two measures:

- *Accuracy of changing robot inference* specifies the inferenc accuracy of the adversary using the threat model described in Eq. (2) to identify the changing robot. Let $\delta = \frac{k}{K}$ represent the number of successful inferences k out of the total simulation runs K.
- *Aggregation ability inference* specifies the aggregation ability of the inferred changing robot. Let $\sqrt{a_c^*}$ represent the inferred aggregation ability, where c is the index of the inferred changing robot, as determined by the threat model in Eq. (3).

We repeat our evaluations 100 times for each value of ϵ in the range [0.01, 1], and summarize the inference results of the adversary under both baseline flocking and private flocking. Fig. 6 shows that under baseline flocking, the adversary using the threat model described in Eq. (1)-(3) can identify the changing robot with 100% accuracy, and has a 0.1% margin of error in inferring the aggregation ability of the changing robot, calculated as $(2103 - 2100)/2100$. Under private flocking, Fig. 6A shows that the adversary can identify the changing robot with 100% accuracy when $\epsilon \geq 0.85$, but with only 6% or less accuracy when $\epsilon \leq 0.13$. The adversary's ability to accurately identify the changing robot decreases as the value of ϵ decreases. We conclude that $\epsilon \leq 0.13$ represents a lower threshold where private information is almost completely protected, while $\epsilon \geq 0.85$ marks an upper threshold where private information cannot be protected at all. Fig. 6B shows that the adversary has a 12% margin of error in inferring the aggregation ability of the changing robot, calculated as $(2100-1844)/2100$. This represents a significant privacy enhancement in terms of aggregation ability. Overall, despite a swarm robotic system using the differentially private mechanism can only reach a relative steady state instead of a stable state using a non-private mechanism, our proposed approach can effectively protect the aggregation ability privacy of individual robots while maintaining a flocking behavior, which is beyond the capacity of the basic flocking control.

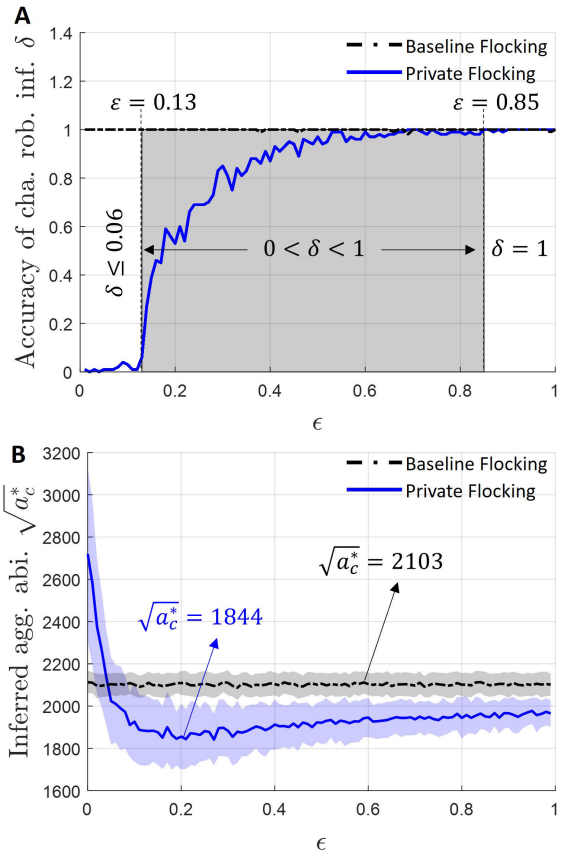


Fig. 6. The effects of the differential privacy parameter ϵ on the adversary's inference results. The effect of successive changes in ϵ on (A) the accuracy of changing robot inference and (B) the aggregation ability inference. $\sqrt{a_c} = 2100$ for the changing robot, $\sqrt{a} = 2000$ for the other robots, and $n = 100$. We take 100 independent runs for each value of $\epsilon = [0.01 : 1]$.

D. Discussion

The aggregation ability privacy in flocking behaviors provides a good opportunity to study differential privacy in swarm robotic systems. Along with privacy concerns resulting from explicit information sharing, such as role privacy, tracking privacy, target privacy, and optimal consensus privacy, the aggregation ability privacy discussed in this work suggests that the swarm's configuration can also reveal sensitive information about each robot's preferences, even when there is no information exchange. This is particularly relevant when tasks require collective motions in a specific formation, such as the uniform distribution. While the notation of differential privacy primarily focuses on concealing the aggregation ability of one robot, we demonstrate that aggregation ability privacy is a more challenging issue when multiple robots have different aggregation abilities than others. Developing a proof for privacy preservation to multiple robots is still an open question.

As shown in Fig. 7, robots with strong aggregation abilities move towards the group center in a flocking system, while those with weak aggregation abilities move towards the boundary. This outcome is independent of the differentially private mechanism used. It suggests that the differentially private mechanism has limitations in protecting a robot group's aggregation abilities. Adversaries can easily identify which group of robots have strong or weak aggregation

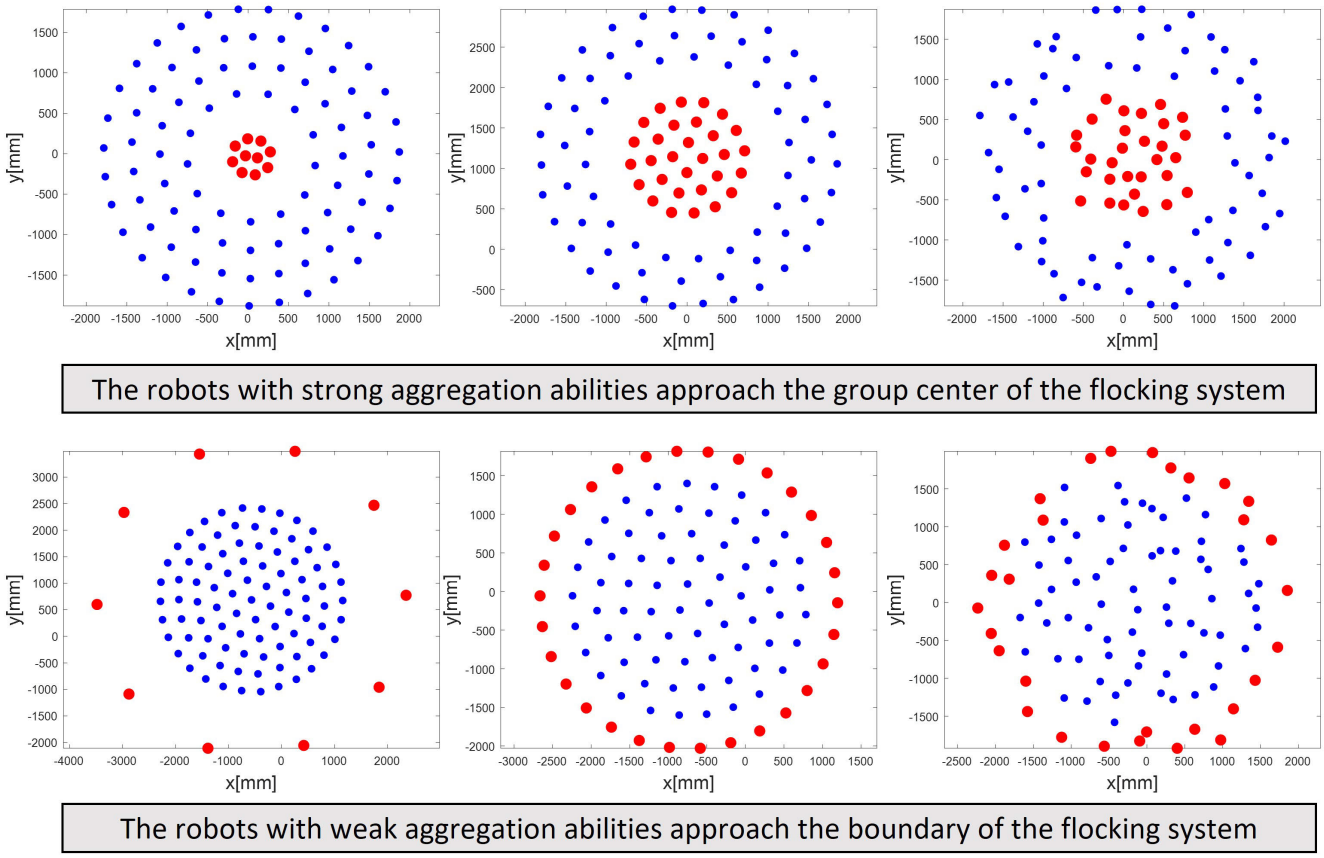


Fig. 7. The configuration of swarm robots reveal sensitive information about the aggregation abilities of robots. Illustrative videos can be found in the supplementary material.

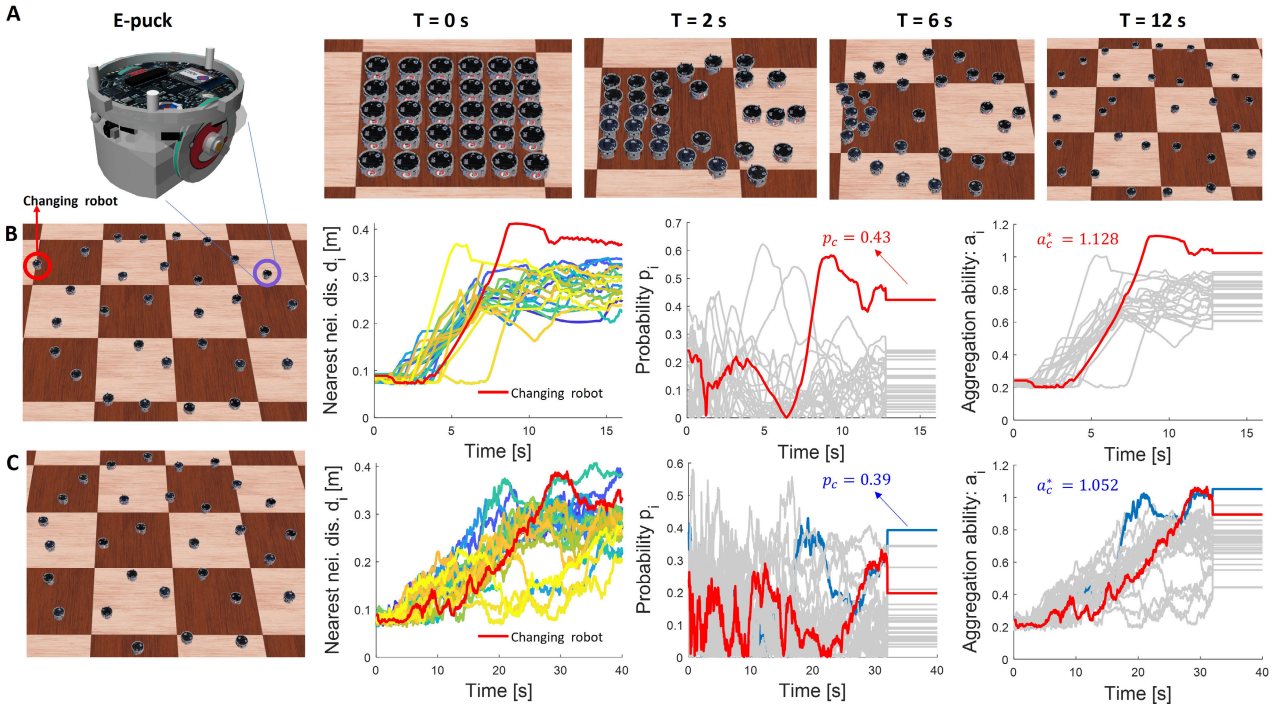


Fig. 8. Experiments using 30 e-puck robots in the Webots simulation environment. (A) Snapshots of one experiment illustrating swarm robotic flocking control. (B) Swarm robotic flocking without the privacy-preserving mechanism. (C) Swarm robotic flocking with the privacy-preserving mechanism. A video of all experiments is available in the supplementary material.

abilities, and to what degree their abilities differ from others. This is a unique problem of aggregation ability privacy in flocking system. To address more general issues concerning role privacy and relative position privacy in swarm robotic systems, more sophisticated privacy-preserving mechanisms may be necessary.

VII. Experiments

We utilized 30 e-puck robots [36] to conduct experiments in the Webots simulation environment [37]. These experiments served as a proof of concept to validate our approach. The e-puck robot operates using a differential-drive platform, controlled by its linear and angular velocities, as detailed in [9], [10]. Key specifications include a diameter of 0.071 meters, a height of 0.050 meters, a wheel radius of 0.020 meters, and an axle length of 0.052 meters. The robot is capable of a maximum forward/backward speed of 0.15 m/s and a maximum rotational speed of 7.536 rad/s. For our experiments, we set $r_0 = 0.2$ m, $r_1 = 0.4$ m, $\epsilon = 0.1$, $\zeta = 0.2$, and $\delta_s = 1$ m. Notably, one robot exhibited a different aggregation ability with $a = 1.200$, while the others were assigned the same value of $a = 1.000$. All robots were initially deployed in a square area of 0.5 m $\times$ 0.5 m for each experimental run. We conducted a series of experiments, all of which produced similar outcomes. The snapshots of one experiment are illustrated in Fig. 8A, where all robots had the same aggregation ability.

Fig. 8B shows the swarm robotic flocking control without a differential privacy mechanism. The results indicate that the nearest neighboring distance of the changing robot can be easily identified, as marked by the red line. The highest degree of deviation ($p_c = 0.43$) precisely points to the changing robot, enabling the adversary to accurately identify it. The inferred value $a_c^* = 1.128$ is close to $a_c = 1.200$, allowing the adversary to correctly infer the aggregation ability of the changing robot.

In contrast, Fig. 8C displays the results with the differential privacy mechanism. The swarm robotic system effectively conceals the changing robot and its aggregation ability. The adversary is unable to correctly identify the changing robot or its corresponding aggregation ability. Specifically, the highest degree of deviation points to a normal robot, and the aggregation ability of the changing robot is incorrectly inferred via this normal robot (indicated by the blue line). Overall, the comparison results of experiments with 30 e-puck robots confirm that our approach effectively maintains the privacy of robots' aggregation abilities throughout the flocking process. A video of all experiments is available in the supplementary material.

VIII. Conclusion and Future Work

This work addresses the problem of swarm robotic flocking and aggregation ability privacy. Our objective is to conceal the private aggregation ability of each robot from adversaries, thereby preventing them from accurately inferring which robot changes its aggregation ability and its corresponding level. To achieve this, we propose a differentially private mechanism based on the Laplace mechanism. The results demonstrate that an adversary's ability to infer the aggregation ability of a changing robot decreases as the value of the differential privacy parameter ϵ decreases. Specifically, $\epsilon \leq 0.13$ represents a lower threshold where private information is almost completely protected, whereas $\epsilon \geq 0.85$ marks an upper threshold where private information cannot be protected at all. Future work will explore differentially private mechanisms for more general problems, including role privacy and relative position privacy in swarm robotic systems.

Appendix

Proof: We take velocity as an example:

$$\begin{aligned}\Delta v(t) &= \max_{A,A'} \|\mathbf{v}(A,t) - \mathbf{v}(A',t)\|_1 \\ &= \max_{i\in\{1,\cdots,n\}} \sum_{i=1}^{n} |\mathbf{v}_i(a_i,t) - \mathbf{v}_i(a_i',t)| \\ &= \max_{k\in\{1,\cdots,n\}} |\mathbf{v}_k(a_k,t) - \mathbf{v}_k(a_k',t)| \end{aligned} \tag{26}$$

It is seen that

$$\begin{aligned}\mathbf{v}_k(a_k,t) &= \mathbf{v}_k(a_k,t-dt) + \mathbf{u}_k(a_k,t)dt \\ \mathbf{v}_k(a_k',t) &= \mathbf{v}_k(a_k',t-dt) + \mathbf{u}_k(a_k',t)dt \end{aligned} \tag{27}$$

Assume that $\mathbf{v}_k(a_k,0) = \mathbf{v}_k(a_k',0)$, then we have

$$\mathbf{v}_k(a_k,t) - \mathbf{v}_k(a_k',t) = \big(\mathbf{u}_k(a_k,t) - \mathbf{u}_k(a_k',t)\big)dt \tag{28}$$

Substitute Eq. (28) into Eq. (26), we then have

$$\begin{aligned}\Delta v(t) &= \max_{k\in\{1,\cdots,n\}} |\mathbf{v}_k(a_k,t) - \mathbf{v}_k(a_k',t)| \\ &= dt \cdot \max_{k\in\{1,\cdots,n\}} |\mathbf{u}_k(a_k,t) - \mathbf{u}_k(a_k',t)| \\ &= \Delta u(t)\cdot dt \end{aligned} \tag{29}$$

A similar proof process can be envisioned when the position is considered for the sensitivity analysis. ■

References

[1] S. Garnier, J. Gautrais, and G. Theraulaz, "The biological principles of swarm intelligence," *Swarm Intell.*, vol. 1, no. 1, pp. 3–31, 2007.

[2] A. J. C. Sharkey, "Robots, insects and swarm intelligence," *Artif. Intell. Rev.*, vol. 26, no. 4, pp. 255–268, Dec. 2006.

[3] B. L. Partridge, "The structure and function of fish schools," *Sci. Amer.*, vol. 246, no. 6, pp. 114–123, Jun. 1982.

[4] S. Zhang, M. Liu, X. Lei, Y. Huang, and F. Zhang, "Multi-target trapping with swarm robots based on pattern formation," *Robot. Auto. Syst.*, vol. 106, pp. 1–13, Aug. 2018.

[5] S. Zhang, M. Liu, X. Lei, P. Yang, Y. Huang, and R. Clark, "Synchronous intercept strategies for a robotic defense-intrusion game with two defenders," *Auto. Robots*, vol. 45, no. 1, pp. 15–30, Jan. 2021.

[6] S. Zhang, X. Lei, Z. Zheng, and X. Peng, "Collective fission behavior in swarming systems with density-based interaction," *Phys. A, Stat. Mech. Appl.*, vol. 603, Oct. 2022, Art. no. 127723.

[7] S. Zhang and J. Pan, "Collecting a flock with multiple sub-groups by using multi-robot system," *IEEE Robot. Autom. Lett.*, vol. 7, no. 3, pp. 6974–6981, Jul. 2022.

[8] X. Lei, S. Zhang, Y. Xiang, and M. Duan, "Self-organized multi-target trapping of swarm robots with density-based interaction," *Complex Intell. Syst.*, vol. 9, no. 5, pp. 5135–5155, Oct. 2023.

[9] S. Zhang, X. Lei, M. Duan, X. Peng, and J. Pan, "A distributed outmost push approach for multirobot herding," *IEEE Trans. Robot.*, vol. 40, pp. 1706–1723, 2024.

[10] S. Zhang, X. Lei, X. Peng, and J. Pan, "Heterogeneous targets trapping with swarm robots by using adaptive density-based interaction," *IEEE Trans. Robot.*, vol. 40, pp. 2729–2748, 2024.

[11] L. Zhou and P. Tokekar, "Multi-robot coordination and planning in uncertain and adversarial environments," *Current Robot. Rep.*, vol. 2, no. 2, pp. 147–157, Apr. 2021.

[12] H. Zheng, J. Panerati, G. Beltrame, and A. Prorok, "An adversarial approach to private flocking in mobile robot teams," *IEEE Robot. Autom. Lett.*, vol. 5, no. 2, pp. 1009–1016, Apr. 2020.

[13] Y. Wang, Z. Huang, S. Mitra, and G. E. Dullerud, "Differential privacy in linear distributed control systems: Entropy minimizing mechanisms and performance tradeoffs," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 118–130, Mar. 2017.

[14] Y. Zhang and D. A. Shell, "Complete characterization of a class of privacy-preserving tracking problems," *Int. J. Robot. Res.*, vol. 38, nos. 2–3, pp. 299–315, Mar. 2019.

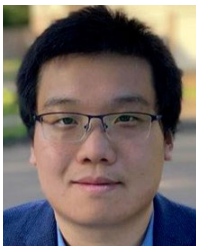
[15] B. Brodt and A. Pierson, "Obscuring objectives with Pareto-optimal privacy-aware trajectories in multi-robot coverage," in *Proc. IEEE Int. Conf. Robot. Autom. (ICRA)*, May 2023, pp. 7670–7676.
[16] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Proc. Theory Cryptogr. Conf.* New York, NY, USA: Springer, 2006, pp. 265–284.
[17] D. Wang, J. Ren, Z. Wang, X. Pang, Y. Zhang, and X. Shen, "Privacy-preserving streaming truth discovery in crowdsourcing with differential privacy," *IEEE Trans. Mobile Comput.*, vol. 21, no. 10, pp. 3757–3772, Oct. 2022.
[18] C. Ma, L. Yuan, L. Han, M. Ding, R. Bhaskar, and J. Li, "Data level privacy preserving: A stochastic perturbation approach based on differential privacy," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 4, pp. 3619–3631, Apr. 2023.
[19] Z. Zheng, T. Wang, A. K. Bashir, M. Alazab, S. Mumtaz, and X. Wang, "A decentralized mechanism based on differential privacy for privacy-preserving computation in smart grid," *IEEE Trans. Comput.*, vol. 71, no. 11, pp. 2915–2926, Nov. 2022.
[20] F. Wang et al., "Privacy-aware traffic flow prediction based on multi-party sensor data with zero trust in smart city," *ACM Trans. Internet Technol.*, vol. 23, no. 3, pp. 1–19, 2023.
[21] M. Adnan, S. Kalra, J. C. Cresswell, G. W. Taylor, and H. R. Tizhoosh, "Federated learning and differential privacy for medical image analysis," *Sci. Rep.*, vol. 12, no. 1, p. 1953, Feb. 2022.
[22] J. Drechsler, "Differential privacy for government agencies—Are we there yet?" *J. Amer. Stat. Assoc.*, vol. 118, no. 541, pp. 761–773, Jan. 2023.
[23] Y. Zhao and J. Chen, "A survey on differential privacy for unstructured data content," *ACM Comput. Surveys*, vol. 54, no. 10, pp. 1–28, 2022.
[24] J. Peng, J. Guo, F. Bao, C. Yang, Y. Xu, and Y. Qin, "Multi-robot privacy-preserving algorithms based on federated learning: A review," *Comput., Mater. Continua*, vol. 77, no. 3, pp. 2971–2994, 2023.
[25] A. Prorok and V. Kumar, "A macroscopic privacy model for heterogeneous robot swarms," in *Proc. 10th Int. Conf.* New York, NY, USA: Springer, Sep. 2016, pp. 15–27.
[26] X. Chen, T. Zhang, S. Shen, T. Zhu, and P. Xiong, "An optimized differential privacy scheme with reinforcement learning in VANET," *Comput. Secur.*, vol. 110, Nov. 2021, Art. no. 102446.
[27] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private distributed convex optimization via functional perturbation," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 1, pp. 395–408, Mar. 2018.
[28] D. Fiore and G. Russo, "Resilient consensus for multi-agent systems subject to differential privacy requirements," *Automatica*, vol. 106, pp. 18–26, Aug. 2019.
[29] T. Dong, H. Zhu, and W. Hu, "Event-trigger optimal consensus for multi-agent system subject to differential privacy," *Int. J. Control, Autom. Syst.*, vol. 19, no. 9, pp. 2940–2949, Sep. 2021.
[30] K. Zhang, Z. Li, Y. Wang, A. Louati, and J. Chen, "Privacy-preserving dynamic average consensus via state decomposition: Case study on multi-robot formation control," *Automatica*, vol. 139, May 2022, Art. no. 110182.
[31] Y.-W. Lv, G.-H. Yang, and C.-X. Shi, "Differentially private distributed optimization for multi-agent systems via the augmented Lagrangian algorithm," *Inf. Sci.*, vol. 538, pp. 39–53, Oct. 2020.
[32] Z. Zhang, H. Zhu, and M. Xie, "Differential privacy may have a potential optimization effect on some swarm intelligence algorithms besides privacy-preserving," *Inf. Sci.*, vol. 654, Jan. 2024, Art. no. 119870.
[33] J. Cortés, G. E. Dullerud, S. Han, J. Le Ny, S. Mitra, and G. J. Pappas, "Differential privacy in control and network systems," in *Proc. IEEE 55th Conf. Decis. Control (CDC)*, Dec. 2016, pp. 4252–4272.
[34] R. C. Fetecau, Y. Huang, and T. Kolokolnikov, "Swarm dynamics and equilibria for a nonlocal aggregation model," *Nonlinearity*, vol. 24, no. 10, pp. 2681–2716, Oct. 2011.
[35] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Found. Trends Theor. Comput. Sci.*, vol. 9, nos. 3–4, pp. 211–407, 2014.
[36] C. M. Cianci, X. Raemy, J. Pugh, and A. Martinoli, "Communication in a swarm of miniature robots: The e-puck as an educational tool for swarm robotics," in *Swarm Robotics*. Berlin, Germany: Springer, 2007, pp. 103–115.
[37] Webots. *Open-Source Mobile Robot Simulation Software*. Accessed: Nov. 20, 2024. [Online]. Available: http://www.cyberbotics.com

Shuai Zhang received the master's and Ph.D. degrees from Northwestern Polytechnical University in 2015 and 2020, respectively.

He was a joint Ph.D. Student with the University of Strathclyde Glasgow, U.K., from 2017 to 2018. He is currently a Post-Doctoral Fellow with the Department of Computer Science, The University of Hong Kong. His current research interests include robotics and autonomous systems, distributed robot systems, swarm robotics, collective behaviors, multi-robot systems, and multi-agent reinforcement learning. He is an Associate Editor of the IEEE International Conference on Robotics and Biomimetics (IEEE ROBIO 2023).

Yunke Huang received the master's and Ph.D. degrees in physics from Northwestern Polytechnical University, China, in 2015 and 2021, respectively.

She was a joint Ph.D. Student with the University of Strathclyde Glasgow, U.K., from 2017 to 2019. She was a Post-Doctoral Research Fellow with the Department of Aerospace and Mechanical Engineering, The Hong Kong University of Science and Technology, from 2021 to 2023. She is currently a Post-Doctoral Research Fellow with the Department of Computer Science, The University of Hong Kong. Her research interests include peridynamics, fracture mechanics, fluid-structure interactions, nondestructive evaluation, and advanced ultrasonic imaging.



Weizi Li received the Ph.D. degree in computer science from the University of North Carolina at Chapel Hill.

He is currently an Assistant Professor with the Min H. Kao Department of Electrical Engineering and Computer Science, The University of Tennessee at Knoxville, Knoxville. Prior to this position, he was an Assistant Professor with the University of Memphis and a Michael Hammer Postdoctoral Fellow with Massachusetts Institute of Technology (MIT). His current research interests include intelligent transportation systems, robotics, machine learning, and multi-agent systems.

Jia Pan (Senior Member, IEEE) received the Ph.D. degree in computer science from the University of North Carolina at Chapel Hill, Chapel Hill, NC, USA, in 2013.

He is currently an Associate Professor with the Department of Computer Science, The University of Hong Kong, Hong Kong. He is also a member with Centre for Garment Production Ltd., Hong Kong. His research interests include robotics and artificial intelligence as applied to autonomous systems, particularly for navigation and manipulation in challenging tasks, such as effective movement in dense human crowds and manipulating deformable objects for garment automation.