

Herding an Adversarial Swarm in an Obstacle Environment

Vishnu S. Chipade and Dimitra Panagou

Abstract—This paper studies a defense approach against a swarm of adversarial agents. We employ a closed formation (‘StringNet’) of defending agents around the adversarial agents to restrict their motion and guide them to a safe area while navigating in an obstacle-populated environment. Control laws for forming the StringNet and guiding it to a safe area are developed, and the stability of the closed-loop system is analyzed formally. The adversarial swarm is assumed to move as a flock in the presence of rectangular obstacles. Simulation results are provided to demonstrate the efficacy of the approach.

I. INTRODUCTION

Swarm technology has seen a rapid growth recently. Safety-critical infrastructure such as government facilities, airports, military bases are at increased risk of being attacked by swarms of adversarial agents (e.g., aerial robots). This creates a need for defending safety-critical infrastructure from attacks of adversarial swarms, particularly in crowded urban areas.

Counteracting an adversarial swarm by means of physical interception [1], [2] in an urban environment may not be desired due to human presence. Under the assumption of risk-averse and self-interested adversarial agents (attackers) that tend to move away from the defending agents (defenders) and from other dynamic objects, herding can be used as an indirect way of guiding the attackers to a safe area.

In this paper, we consider a problem of defending a safety-critical area (protected area) from an adversarial swarm. We address this as a problem of herding a swarm of attackers to a safe area, while avoiding the static rectangular obstacles of the urban environment.

The herding approach to herd a flock of birds away from an airport in [3] uses an n -wavefront algorithm, where the motion of the birds on the boundary of the flock is influenced based on the locations of the airport and the safe area. Stability and performance guarantees under directed star communication graph are provided in [4], and experimental results in [5]. In [6] a circular arc formation of herders is used to influence the nonlinear dynamics of the herd based on a potential-field approach. The authors design a point-offset controller to guide the

herd close to a specified location. In [7], biologically-inspired strategies are developed for confining a group of mobile robots. The authors develop strategies based on the “wall” and “encirclement” methods that dolphins use to capture a school of fish. Regions from which this confinement is possible are also derived; however, the results are limited to constant velocity motions. A similar approach of herding by caging is adopted in [8], where a cage of high potential is formed around the sheep (attackers). An RRT approach is used to find a motion plan for the agents while maintaining the cage. However, the formation is assumed to have been already formed around the sheep. Furthermore, the caging of the sheep is only ensured with constant velocity motion under additional conservative assumptions on the distances between the agents. In general, most of these works lack a proper modeling of the adversarial agents’ intent to reach or attack a certain protected area.

In [9], [10] the authors discuss herding using a switched systems approach; the herder (defender) chases targets (attackers) sequentially by switching among them so that certain dwell-time conditions are satisfied to guarantee stability of the resulting trajectories. However, the assumption that only one of the targets is influenced by the herder at any time is conservative for the problem of defending against a swarm of attackers. The authors in [11] use approximate dynamic programming to obtain near-optimal control policies for the herder to chase a target agent to a goal location.

The aforementioned approaches assume some form of potential field to model the repulsion of the attackers from the defenders, and develop herding strategies for the defenders based on this potential field. Hence, such approaches may fail to create a proper potential barrier around the attackers if the potential field of the attackers is unknown to defenders, or is modeled inaccurately. In addition, most of the earlier work does not consider obstacles in the environment. In our prior work [12], we developed a strategy for herding a single attacker to a safe area in the presence of rectangular obstacles.

In this paper, we propose what we call ‘StringNet Herding’, in which a closed formation of physical strings called ‘StringNet’ is formed by the defenders around the swarm of attackers. It is assumed that the string between two defenders serves as a barrier through which the attackers cannot escape. The StringNet is controlled collectively to herd the swarm of attackers. The proposed approach only assumes that the attackers avoid collisions with defenders and barriers, while the control actions of

The authors are with the Department of Aerospace Engineering, University of Michigan, Ann Arbor, MI, USA; (vishnuc,dpanagou}@umich.edu

This work has been funded by the Center for Unmanned Aircraft Systems (C-UAS), a National Science Foundation Industry/University Cooperative Research Center (I/UCRC) under NSF Award No. 1738714 along with significant contributions from C-UAS industry members.

the attackers are not known a priori. To demonstrate the proposed approach, we use flocking behavior for the attackers, which however is not known to the defenders.

We build on earlier work [13]–[17] to develop a flocking controller for the attackers in the presence of rectangular obstacles. The controller uses the β -agent strategy [14], [15], in which a virtual agent called β -agent is assumed to move on the boundary of the obstacle, and the control action is designed to maintain a certain distance from this β -agent using a potential function approach. We generate β -agents along a superelliptic curve that is at least C^1 around the rectangular obstacles. Also, in contrast to earlier work [6], [8] that treats robots as point masses, we assume agents with known circular footprints. Furthermore, no constant velocity assumption is made about the attackers as is done in [7], [8].

In summary, the novelties and the contributions are: (i) A ‘StringNet’ formation to restrict the motion of the attackers inside the StringNet and to herd them towards a safe area. We develop provably-correct control laws for the defenders to form the StringNet in finite time, and to herd the entrapped attackers to safe area. (ii) The definition of β -agents along superelliptic contours around rectangular obstacles with C^1 velocity profile for obstacle avoidance in flocking.

The rest of the paper is structured as follows: Section II describes the mathematical modeling and problem statement. The flocking and herding algorithms are discussed in Section III and IV, while simulations are provided in Section V. The conclusions and the ongoing work are discussed in Section VI.

II. MODELING AND PROBLEM STATEMENT

Notation: Vectors and matrices are denoted by small and capital bold letters, respectively (e.g., \mathbf{r} , \mathbf{P}). Script letters denote sets (e.g., \mathcal{P}). $\|\cdot\|$ denotes Euclidean norm of its argument. $|\cdot|$ denotes absolute value of a scalar argument and cardinality if the argument is a set. The function sig^α is defined as: $\text{sig}^\alpha(\mathbf{x}) = \mathbf{x} \|\mathbf{x}\|^{\alpha-1}$. $\mathbb{R}_{\geq 0} = \{x \in \mathbb{R} | x \geq 0\}$. $R_i^j = \|\mathbf{r}_i - \mathbf{r}_j\|$ and E_{ok}^i are the Euclidean distance between object j and i , and the Super-elliptic distance between i and \mathcal{O}_k , respectively. A blending function [18], $\sigma_i^j(\delta)$, characterized by a doublet $(\bar{\delta}_i^j, \bar{\delta}_i^j)$ with $\bar{\delta}_i^j < \bar{\delta}_i^j$ is defined as:

$$\sigma_i^j(\delta) = \begin{cases} 1, & \delta \leq \bar{\delta}_i^j; \\ A_i^j \delta^3 + B_i^j \delta^2 + C_i^j \delta + D_i^j, & \bar{\delta}_i^j \leq \delta \leq \bar{\delta}_i^j; \\ 0, & \delta \geq \bar{\delta}_i^j; \end{cases} \quad (1)$$

where δ is the distance between the objects i and j . The coefficients $A_i^j, B_i^j, C_i^j, D_i^j$ are chosen as: $A_i^j = \frac{2}{(\bar{\delta}_i^j - \bar{\delta}_i^j)^3}$, $B_i^j = \frac{-3(\bar{\delta}_i^j + \bar{\delta}_i^j)}{(\bar{\delta}_i^j - \bar{\delta}_i^j)^3}$, $C_i^j = \frac{6\bar{\delta}_i^j \bar{\delta}_i^j}{(\bar{\delta}_i^j - \bar{\delta}_i^j)^3}$, $D_i^j = \frac{(\bar{\delta}_i^j)^2(\bar{\delta}_i^j - 3\bar{\delta}_i^j)}{(\bar{\delta}_i^j - \bar{\delta}_i^j)^3}$, so that (1) is a C^1 function. The argument δ is either the Euclidean distance or the Super-elliptic distance, depending on the objects under consideration, and will be omitted when clear from the context.

We consider N_a attackers \mathcal{A}_i , $i \in I_a = \{1, 2, \dots, N_a\}$ and N_d defenders \mathcal{D}_j , $j \in I_d = \{1, 2, \dots, N_d\}$, operating in a 2D environment $\mathcal{W} \subseteq \mathbb{R}^2$ with N_o rectangular obstacles, a protected area $\mathcal{P} \subset \mathcal{W}$ defined as $\mathcal{P} = \{\mathbf{r} \in \mathbb{R}^2 \mid \|\mathbf{r} - \mathbf{r}_p\| \leq \rho_p\}$, and a safe area $\mathcal{S} \subset \mathcal{W}$, defined as $\mathcal{S} = \{\mathbf{r} \in \mathbb{R}^2 \mid \|\mathbf{r} - \mathbf{r}_s\| \leq \rho_s\}$, where (\mathbf{r}_p, ρ_p) and (\mathbf{r}_s, ρ_s) are the centers and radii of the corresponding areas, respectively. The agents \mathcal{A}_i and \mathcal{D}_j are modeled as discs of radii ρ_a and $\rho_d \leq \rho_a$, respectively and have Double Integrator (DI) dynamics with a linear drag term:

$$\dot{\mathbf{r}}_{ai} = \mathbf{v}_{ai}, \quad \dot{\mathbf{v}}_{ai} = \mathbf{u}_{ai} - C_d \mathbf{v}_{ai}; \quad (2)$$

$$\dot{\mathbf{r}}_{dj} = \mathbf{v}_{dj}, \quad \dot{\mathbf{v}}_{dj} = \mathbf{u}_{dj} - C_d \mathbf{v}_{dj}; \quad (3)$$

where C_d is a drag coefficient, for $i = ai$ and $i = dj$ $\mathbf{r}_i = [x_i \ y_i]^T$, $\mathbf{v}_i = [v_{x_i} \ v_{y_i}]^T$ are position and velocity of \mathcal{A}_i and \mathcal{D}_j , respectively, and $\mathbf{u}_i = [u_{x_i} \ u_{y_i}]^T$ is acceleration input (control input) of \mathcal{A}_i and \mathcal{D}_j , respectively. We assume that the control action of \mathcal{A}_i satisfies $\|\mathbf{u}_{ai}\| < u_{ma}$. This model poses a realistic speed bound on each attacker with limited acceleration control, i.e., $v_{ai} = \|\mathbf{v}_{ai}\| < v_{ma} = \frac{u_{ma}}{C_d}$. We assume that every defender \mathcal{D}_j senses the position \mathbf{r}_{ai} and velocity \mathbf{v}_{ai} of the attacker \mathcal{A}_i when \mathcal{A}_i is inside a circular sensing-zone $\mathcal{Z}_d^s = \{\mathbf{r} \in \mathbb{R}^2 \mid \|\mathbf{r} - \mathbf{r}_p\| \leq \rho_d^s\}$ around \mathcal{P} . Each attacker \mathcal{A}_i has a similar local sensing zone $\mathcal{Z}_{ai}^s = \{\mathbf{r} \in \mathbb{R}^2 \mid \|\mathbf{r} - \mathbf{r}_{ai}\| \leq \rho_{ai}^s\}$.

We consider static obstacles \mathcal{O}_k of rectangular shape, with their edges along the x -axis ($\hat{\mathbf{i}}$) and y -axis ($\hat{\mathbf{j}}$) of a coordinate frame \mathcal{F}_{gi} , defined as:

$$\mathcal{O}_k = \{\mathbf{r} \in \mathbb{R}^2 \mid |x - x_{ok}| \leq \frac{w_{ok}}{2}, |y - y_{ok}| \leq \frac{h_{ok}}{2}\}, \quad (4)$$

where $\mathbf{r}_{ok} = [x_{ok} \ y_{ok}]^T$ is the center, w_{ok} and h_{ok} are the lengths along $\hat{\mathbf{i}}$ and $\hat{\mathbf{j}}$ of \mathcal{O}_k for all $k \in I_o = \{1, 2, \dots, N_o\}$.

The attackers aim to reach the protected area \mathcal{P} as a flock, and the defenders aim to herd the flock to the safe area \mathcal{S} before it reaches \mathcal{P} . Formally, we consider the following two problems.

Problem 1 (Flocking): Design control actions \mathbf{u}_{ai} , $\forall i \in I_a$ such that \mathcal{A} ’s reach \mathcal{P} as a flock formation while avoiding the static rectangular obstacles.

Problem 2 (Herding): Find control actions \mathbf{u}_{dj} , $\forall j \in I_d$ to accomplish: 1) StringNet formation around the swarm of attackers in finite time. 2) Once the StringNet is formed, move the StringNet to the safe area \mathcal{S} while avoiding the obstacles \mathcal{O}_k .

III. FLOCKING

The neighboring graph [17] for the attackers is denoted as $\mathcal{G}_a = (\mathcal{V}_a, \mathcal{E}_a)$, where $\mathcal{V}_a = \{\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_{N_a}\}$ is the set of vertices and \mathcal{E}_a is the set of edges. Each attacker \mathcal{A}_i communicates with its neighbors $\mathcal{N}_{ai}^a = \{i' \in \mathcal{V}_a \mid (\mathcal{A}_i, \mathcal{A}_{i'}) \in \mathcal{E}_a\}$. We define a potential function $V_i^j : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$ as:

$$V_i^j(R_i^j) = \ln \left(\frac{\tilde{R}_i^j}{R_i^j - \hat{R}_i^j} + \frac{R_i^j - \hat{R}_i^j}{\tilde{R}_i^j} \right), \quad (5)$$

where $\tilde{R}_i^j > \hat{R}_i^j$ is the desired distance between agent i and agent j , and \hat{R}_i^j is the minimum safety distance between agent i and agent j . We have that as R_i^j approaches \hat{R}_i^j , the potential V_i^j tends to ∞ . A control action corresponding to V_i^j is defined as:

$$\mathbf{u}_p(\mathbf{x}_i^j) = -\zeta_i^j(\mathbf{v}_i - \mathbf{v}_j) - \mu_i^j \cdot \nabla_{\mathbf{r}_i} V_i^j \quad (6)$$

where $\mathbf{x}_i^j = [\mathbf{r}_i^T, \mathbf{v}_i^T, \mathbf{r}_j^T, \mathbf{v}_j^T]^T$, ζ_i^j and μ_i^j are control gains.

The swarm of attackers aims to reach the protected area \mathcal{P} while avoiding the static obstacles \mathcal{O}_k and maintaining a flock described by potential functions $V_{ai}^{ai'}$ for all $i, i' \in I_a$ over the graph \mathcal{G}_a . The control action for the flock of the attackers is defined as [17], [19]:

$$\mathbf{u}_{ai}^f = k_a^r(\mathbf{r}_p - \mathbf{r}_{ai}) + \sum_{i' \in \mathcal{N}_{ai}^a} \mathbf{u}_p(\mathbf{x}_{ai}^{ai'}) + \sum_{k \in \mathcal{N}_{ai}^o} \sigma_{ai}^{ok} \cdot \mathbf{u}_p(\mathbf{x}_{ai}^{\beta ik}) \quad (7)$$

where $\mathbf{x}_{ai}^{\beta ik} = [\mathbf{r}_{ai}^T, \mathbf{v}_{ai}^T, \mathbf{r}_{\beta ik}^T, \mathbf{v}_{\beta ik}^T]^T$, where $\mathbf{r}_{\beta ik}$ and $\mathbf{v}_{\beta ik}$ is the position and velocity of the β -agent on the boundary of \mathcal{O}_k corresponding to \mathcal{A}_i that is used for avoiding \mathcal{O}_k . The blending function σ_{ai}^{ok} allows smooth transition to the obstacle avoidance part of the controller, and is characterized by the doublet $(\xi_a^o, \bar{\xi}_a^o)$. \mathcal{N}_{ai}^o is a set of neighboring obstacles defined as: $\mathcal{N}_{ai}^o = \{k \in I_o | \sigma_{ai}^{ok} > 0\}$. The center \mathbf{r}_p of the protected area \mathcal{P} acts as a γ -agent [15] providing navigational feedback.

A. β -agents around Rectangular Obstacles

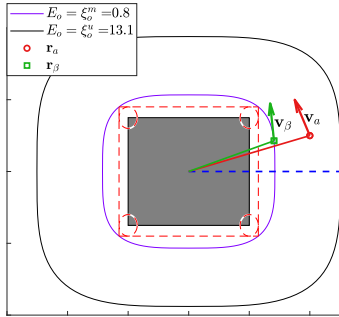


Fig. 1: β -agent around rectangles for obstacle avoidance

The superelliptic distance E_{ok} is defined as:

$$E_{ok} = \left| \frac{x - x_{ok}}{a_{ok}} \right|^{2n_{ok}} + \left| \frac{y - y_{ok}}{b_{ok}} \right|^{2n_{ok}} - 1. \quad (8)$$

The projection $\mathbf{r}_{\beta ik}$ of \mathbf{r}_{ai} on the \mathcal{SE}_{ok} is the closest point on \mathcal{SE}_{ok} such that the unit tangent $\hat{\mathbf{t}}_{ok}(\mathbf{r}_{\beta ik})$ to \mathcal{SE}_{ok} at $\mathbf{r}_{\beta ik}$ is normal to $\mathbf{r}_{ai} - \mathbf{r}_{\beta ik}$, and is found by solving:

$$\left| \frac{x_{\beta ik} - x_{ok}}{a_{ok}} \right|^{2n_{ok}} + \left| \frac{y_{\beta ik} - y_{ok}}{b_{ok}} \right|^{2n_{ok}} - 1 = \xi_{ok}^m, \quad (9a)$$

$$-\frac{b^{2n_{ok}} \text{sig}^{2n_{ok}-2}(x_{\beta ik} - x_{ok})}{a^{2n_{ok}} \text{sig}^{2n_{ok}-2}(y_{\beta ik} - y_{ok})} \cdot \frac{y_{\beta ik} - y_{ai}}{x_{\beta ik} - x_{ai}} = -1. \quad (9b)$$

where $\text{sig}^m(x) = x|x|^m$. Fig. 1 shows the projection $\mathbf{r}_{\beta ik}$ (green square) of \mathbf{r}_{ai} (red circle). The velocity $\mathbf{v}_{\beta ik}$ can be then obtained as: $\mathbf{v}_{\beta ik} = (\mathbf{v}_{ai} \cdot \hat{\mathbf{t}}_{ok}(\mathbf{r}_{\beta ik})) \hat{\mathbf{t}}_{ok}(\mathbf{r}_{\beta ik})$.

B. Avoiding Dynamic Obstacles during Flocking

1) *Avoiding the Defenders*: In addition to avoiding static obstacles, the attackers apply the following control action to avoid the defenders:

$$\mathbf{u}_{ai}^d = \sum_{j \in \mathcal{N}_{ai}^d} \sigma_{ai}^{dj} \cdot \mathbf{u}_p(\mathbf{x}_{ai}^{dj}), \quad (10)$$

where σ_{ai}^{dj} is characterized by the doublet (R_a^d, \bar{R}_a^d) . \mathcal{N}_{ai}^d is a set of defenders in the sensing zone of \mathcal{A}_i defined as: $\mathcal{N}_{ai}^d = \{j \in I_d | R_{ai}^{dj} < \rho_{ai}^s\}$, and $\tilde{R}_{ai}^{dj} > \bar{R}_a^d$.

2) *Avoiding the Strings*: The strings (string barriers) are line segments between defenders. The attackers can sense these strings in their sensing zone and react to them using the control action:

$$\mathbf{u}_{ai}^b = \sum_{s \in \mathcal{N}_{ai}^b} \sigma_{ai}^{bs} \cdot \mathbf{u}_p(\mathbf{x}_{ai}^{bs}), \quad (11)$$

where \mathbf{u}_p is given by (6) and V_{ai}^{bs} is a potential function for \mathcal{A}_i corresponding to its projection $(\mathbf{r}_{bs}, \mathbf{v}_{bs})$ on the string barrier \mathcal{B}_s (Fig. 2). σ_{ai}^{bs} and \mathcal{N}_{ai}^b are defined similar to σ_{ai}^{dj} and \mathcal{N}_{ai}^d . The combined bounded control action for the attackers' flock is given as:

$$\mathbf{u}_{ai} = \sigma_a \left(\mathbf{u}_{ai}^f + \mathbf{u}_{ai}^d + \mathbf{u}_{ai}^b + C_d \mathbf{v}_{ai} \right), \quad (12)$$

where saturation function $\sigma_a(\mathbf{u}) = \min(u_{ma}, \|\mathbf{u}\|) \frac{\mathbf{u}}{\|\mathbf{u}\|}$.

Remark 1: The convergence analysis for flocking of the attackers under the control (7) is provided in [14], [15], [17] when the first term is absent i.e. no navigational control command. Similar analysis can be done for the flock's convergence to \mathbf{r}_p . Since flocking is not the focus of this paper we omit the analysis in the interest of space.

IV. HERDING

To herd the flock of attackers to \mathcal{S} , we propose 'StringNet Herding'. StringNet is a closed net of strings formed by the defenders as shown in Fig. 2. The strings can be actual physical strings (ropes) or some mechanism that does not allow the attackers to pass through them. It is assumed that even after being connected by the strings, the motion of defenders is not restricted. The underlying graph structure for the 'StringNet' is defined as:

Definition 1 (StringNet): The StringNet $\mathcal{G}^s = (\mathcal{V}^s, \mathcal{E}^s)$ is a cycle graph consisting of: 1) the defenders as the vertices, $\mathcal{V}^s = \{\mathcal{D}_1, \mathcal{D}_2, \dots, \mathcal{D}_{N_d}\}$, 2) a set of edges, $\mathcal{E}^s = \{(\mathcal{D}_j, \mathcal{D}_{j'}) \in \mathcal{V}^s \times \mathcal{V}^s | \mathcal{D}_j \xleftrightarrow{s} \mathcal{D}_{j'}\}$. The operator \xleftrightarrow{s} denotes a physical string barrier between the defenders.

The StringNet herding consists of three phases: 1) Gathering, 2) StringNet formation and 3) Herding the StringNet to \mathcal{S} . These phases are discussed as follows.

A. Gathering

Once the adversarial attackers are sensed in the sensing zone \mathcal{Z}_d^s , the defenders are tasked to herd them. The defenders first converge to an open semicircular formation in the expected path of the attackers (shortest path for the attackers) and establish strings such that \mathcal{A}_i is connected to \mathcal{A}_{i+1} by a string for all $i = \{1, 2, \dots, N_d - 1\}$

(Fig. 2). The desired position ξ_{dj}^g of \mathcal{D}_j on the stationary semicircular formation \mathcal{F}_d^g (Fig. 2) is designed as:

$$\xi_{dj}^g = \mathbf{r}_{df}^g + \rho_{df}^s \hat{\mathbf{o}}(\theta_{dj}), \text{ where } \theta_{dj} = \theta_{df}^{g*} + \frac{\pi(j-1)}{N_d-1}, \quad (13)$$

where $\hat{\mathbf{o}}(\theta) = \begin{bmatrix} \cos(\theta) \\ \sin(\theta) \end{bmatrix}$ is the unit vector making an angle θ with x -axis, $\mathbf{r}_{df}^g = \rho_{df}^g \hat{\mathbf{o}}(\theta_{ac}^*)$ is a location such that $\rho_{df}^g > \rho_p + d_{ac}^{max}$, where d_{ac}^{max} is the maximum distance attacker's center of mass (ACoM, $\mathbf{r}_{ac} = \frac{1}{N_a} \sum_i \mathbf{r}_{ai}$) can travel towards \mathcal{P} during the StringNet formation phase, discussed next, and $\theta_{df}^{g*} = \theta_{ac}^* - \frac{\pi}{2}$, where θ_{ac}^* is the expected direction of motion of the ACoM on the shortest path from the initial position of ACoM to \mathcal{P} . We have $\xi_{dj}^g = \eta_{dj}^g = \mathbf{0}$ and $\dot{\eta}_{dj}^g = \mathbf{0}$. We assume the following.

Assumption 1: (a) The desired position of \mathcal{D}_j , ξ_{dj}^g , is such that $E_{ok}^{dj,des} > \bar{\xi}_d, \forall j \in I_d, \forall k \in I_o$, where $E_{ok}^{dj,des}$ is super-elliptic distance between ξ_{dj}^g and the obstacle \mathcal{O}_k .

(b) $\rho_{df}^s \sqrt{2 - 2 \cos\left(\frac{\pi}{N_d-1}\right)} > \bar{R}_d^d, \rho_{df}^s > \rho_{ac} + \bar{R}_d^{sc}$ where \bar{R}_d^d and \bar{R}_d^{sc} are the parameters of the blending functions $\sigma_{dj}^{dj'}$ and $\sigma_{dj}^{\delta cj}$ respectively.

To converge to ξ_{dj}^g , a finite-time stabilizing controller is defined as:

$$\mathbf{u}_{dj} = \mathbf{u}_{dj}^0 + \mathbf{u}_{dj}^{col} + \dot{\eta}_{dj}^g, \quad (14)$$

where

$$\begin{aligned} \mathbf{u}_{dj}^0 &= C_d \mathbf{v}_{dj} - k_2 \mathbf{sig}^{\alpha_2}(\mathbf{v}_{dj} - \eta_{dj}^g) - k_1 \mathbf{sig}^{\alpha_1}(\mathbf{r}_{dj} - \xi_{dj}^g) \\ \mathbf{u}_{dj}^{col} &= \sum_{j' \in \mathcal{N}_{dj}^d} \sigma_{dj}^{dj'} \cdot \mathbf{u}_p(\mathbf{x}_{dj}^{dj'}) + \sum_{k \in \mathcal{N}_{dj}^o} \sigma_{dj}^{\delta jk} \cdot \mathbf{u}_p(\mathbf{x}_{dj}^{\delta jk}) \end{aligned} \quad (15)$$

where $k_1, k_2 > 0$. $\mathbf{x}_{dj}^{\delta jk} = [\mathbf{r}_{dj}^T, \mathbf{v}_{dj}^T, \mathbf{r}_{\delta jk}^T, \mathbf{v}_{\delta jk}^T]$, where $\mathbf{r}_{\delta jk}$ and $\mathbf{v}_{\delta jk}$ are the position and the velocity of a virtual δ -agent, similar to β -agent, corresponding to \mathcal{D}_j around the obstacle \mathcal{O}_k . $V_{dj}^{dj'}$, $V_{dj}^{\delta jk}$ are potential functions to avoid collision, respectively, with $\mathcal{D}_{j'}$ and δ -agent on the boundary of \mathcal{O}_k . We have $\bar{R}_{dj}^{dj'} > \bar{R}_d^d$ and $\bar{R}_{dj}^{\delta jk} > \bar{R}_d^d$ to ensure collision avoidance for \mathcal{D}_j .

B. StringNet Formation

The attackers are assumed to stay within a connectivity region of radius ρ_{ac} ($< \rho_{sn}^{max}$) around ACoM. Once the semicircular formation is in place, the defenders wait until attackers come close, i.e., $\|\mathbf{r}_{df}^g - \mathbf{r}_{ac}\| < \epsilon$, where ϵ is a small number. To trap the attackers inside StringNet, a desired regular-polygon formation is designed around the connectivity region of the attackers as shown in Fig. 2. The defenders start tracking their desired positions around the attackers and once \mathcal{D}_1 and \mathcal{D}_{N_d} reach within b_d distance from their respective desired positions they get connected via a string. The desired position ξ_{dj}^s of \mathcal{D}_j on the StringNet \mathcal{G}^s (Fig. 2) is chosen on the circle with radius ρ_{sn} centered at \mathbf{r}_{ac} as:

$$\xi_{dj}^s = \mathbf{r}_{ac} + \rho_{sn} \hat{\mathbf{o}}(\theta_{dj}), \text{ where } \theta_{dj} = \theta_{df}^{s*} + \frac{\pi(2j-1)}{N_d}, \quad (16)$$

for all $j \in I_d$, where $\theta_{df}^{s*} = \theta_{df}^{g*}$. The radius ρ_{sn} should satisfy, $\rho_{ac} + b_d < \rho_{sn} \leq \rho_{sn}^{max} - b_d$, where ρ_{sn}^{max} is the maximum footprint of a formation that can pass through the obstacle-free space in the environment. The

parameter b_d is the maximum position tracking error when the defenders converge to the StringNet formation as obtained in Theorem 1. We have $\xi_{dj}^s = \eta_{dj}^s = \mathbf{r}_{ac} = \mathbf{v}_{ac}$. The control action for \mathcal{D}_j during this phase is:

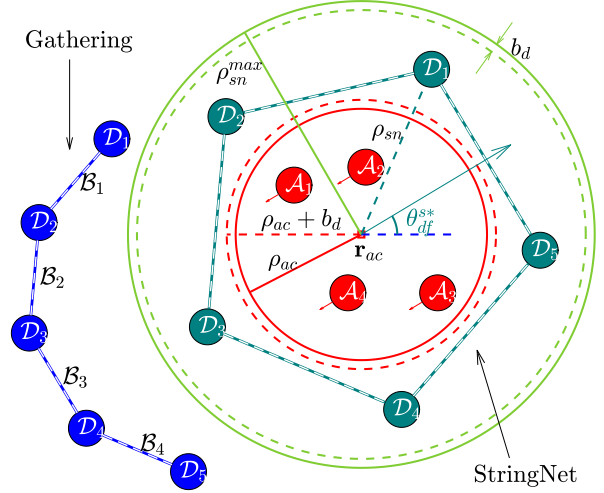


Fig. 2: Desired Positions of the Defenders

$$\begin{aligned} \mathbf{u}_{dj} &= C_d \mathbf{v}_{dj} - k_2 \cdot (\mathbf{v}_{dj} - \eta_{dj}^s) - k_1 \cdot (\mathbf{r}_{dj} - \xi_{dj}^s) \\ &\quad + \sigma_{dj}^{\delta cj} \cdot \mathbf{u}_p(\mathbf{x}_{dj}^{\delta cj}) + \mathbf{u}_{dj}^{col}, \end{aligned} \quad (17)$$

where $\mathbf{r}_{\delta cj}$ and $\mathbf{v}_{\delta cj}$ are the position and the velocity of the δ -agent corresponding to the \mathcal{D}_j on the boundary of the connectivity region of the attackers. The StringNet is achieved when $\|\mathbf{r}_{dj} - \xi_{dj}^s\| \leq b_d$ for all $j \in I_d$ during this phase. To ensure enough space for the movement of the attackers inside the StringNet, the minimum number of defenders require to herd the given number of attackers with connectivity region of radius ρ_{ac} is:

$N_d^{min} = \left\lceil \frac{\pi}{\cos^{-1}\left(\frac{\rho_{ac} + b_d}{\rho_{sn}^{max} - b_d}\right)} \right\rceil$, where $\lceil \cdot \rceil$ gives the smallest integer greater than or equal to its argument.

C. Herding: Moving the StringNet to safe area

Once the defenders form a StringNet around the attackers, they move while tracking a desired rigid closed formation \mathcal{F}_d^h centered at a virtual agent \mathbf{r}_{df} . The virtual agent's dynamics are governed by the DI dynamics similar to (3) with acceleration,

$$\mathbf{u}_{df} = \sigma_{dh} \left(-k_1(\mathbf{r}_{df} - \mathbf{r}_s) + \sum_{k \in \mathcal{N}_{df}^o} \sigma_{df}^{\delta fk} \mathbf{u}_p(\mathbf{x}_{df}^{\delta fk}) \right), \quad (18)$$

where δfk refers to the δ -agent on the obstacle \mathcal{O}_k corresponding to virtual agent at \mathbf{r}_{df} , and $\sigma_{dh}(\mathbf{u}) = \min(u_{md}^h, \|\mathbf{u}\|) \frac{\mathbf{u}}{\|\mathbf{u}\|}$. We choose $u_{md}^h < u_{ma}$ to ensure that the attackers are able to react to the motion of the defenders. The desired positions ξ_{dj}^h of the defenders on the desired closed formation \mathcal{F}_d^h satisfy:

$$\begin{aligned} \xi_{dj}^h &= \eta_{dj}^h, \quad \dot{\eta}_{dj}^h = \mathbf{u}_{df} - C_d \mathbf{v}_{df}; \\ \xi_{dj}^h &= \mathbf{r}_{df} + \rho_{sn} \hat{\mathbf{o}}(\theta_{dj}), \text{ where } \theta_{dj} = \theta_{df}^{s*} + \frac{\pi(2j-1)}{N_d}. \end{aligned} \quad (19)$$

The control (14) is appropriately modified to track $(\xi_{dj}^h, \eta_{dj}^h)$ by replacing $\xi_{dj}^s, \eta_{dj}^s, \dot{\eta}_{dj}^s$ by $\xi_{dj}^h, \eta_{dj}^h, \dot{\eta}_{dj}^h$, respectively.

D. Convergence Analysis

Theorem 1: The StringNet \mathcal{G}^s centered at \mathbf{r}_{ac} is formed around the attackers in finite time from almost all initial conditions under the control action in (14) (gathering phase) and (17) (StringNet formation phase), while avoiding collisions.

Proof: For almost all initial conditions¹ such that $R_{dj}^{dj'} > \hat{R}_{dj}^{dj'}$, we have $\frac{\partial V_{dj}^{dj'}}{\partial R_{dj}^{dj'}} \rightarrow \infty$ as $R_{dj}^{dj'} \rightarrow \hat{R}_{dj}^{dj'}$ implying infinite acceleration applied on \mathcal{D}_j in the direction away from \mathcal{D}_j' which ensures $R_{dj}^{dj'} > \hat{R}_{dj}^{dj'}$ at all times and hence ensures no collision among the defenders. A similar argument can be used to show obstacle avoidance.

During the gathering phase, when the defenders are not in conflict with other defenders or obstacle (i.e., $\sigma_{dj}^{dj'} = \sigma_{dj}^{\delta jk} = 0, \forall j, j' \in I_d; k \in I_o$), the dynamics read:

$$\begin{aligned} \dot{\mathbf{r}}_{dj} &= \mathbf{v}_{dj} \\ \dot{\mathbf{v}}_{dj} &= -k_2 \mathbf{sig}^{\alpha_2}(\mathbf{v}_{dj} - \boldsymbol{\eta}_{dj}^g) - k_1 \mathbf{sig}^{\alpha_1}(\mathbf{r}_{dj} - \boldsymbol{\xi}_{dj}^g) \end{aligned} \quad (20)$$

The origin $\mathbf{r}_{dj} - \boldsymbol{\xi}_{dj}^g = \mathbf{v}_{dj} = \mathbf{0}$ of (20) is finite-time stable [21] if $\alpha_1 = \frac{\alpha_2}{2-\alpha_2}$. Let the convergence time be T_d^g .

Similarly during the StringNet formation phase, when \mathcal{D}_j is not in conflict with any other defenders or obstacle, the error dynamics read:

$$\dot{\mathbf{e}}_{dj} = \begin{bmatrix} \dot{\mathbf{e}}_{dj}^r \\ \dot{\mathbf{e}}_{dj}^v \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -k_1 & -k_2 \end{bmatrix} \begin{bmatrix} \mathbf{e}_{dj}^r \\ \mathbf{e}_{dj}^v \end{bmatrix} + \begin{bmatrix} 0 \\ \dot{\boldsymbol{\eta}}_{dj}^s \end{bmatrix} = \mathbf{A} \mathbf{e}_{dj} + \mathbf{g}_{dj} \quad (21)$$

where $\mathbf{e}_{dj}^r = \mathbf{r}_{dj} - \boldsymbol{\xi}_{dj}^s$, $\mathbf{e}_{dj}^v = \mathbf{v}_{dj} - \boldsymbol{\eta}_{dj}^s$, and $\|\dot{\boldsymbol{\eta}}_{dj}^s\| = \|\dot{\mathbf{v}}_{ac}\| \leq u_{ma}$ which implies the disturbance term \mathbf{g}_{dj} is bounded: $\|\mathbf{g}_{dj}\| \leq u_{ma}$. The nominal system in (21), $\dot{\mathbf{e}}_{dj} = \mathbf{A} \mathbf{e}_{dj}$, is exponentially stable for $k_1, k_2 > 0$. From Theorem 4.6 in [22], there exists a positive definite matrix \mathbf{P} that satisfies the Lyapunov equation $\mathbf{A}^T \mathbf{P} + \mathbf{P} \mathbf{A} = -\mathbf{Q}$, for any given positive definite matrix \mathbf{Q} . The Lyapunov function $V_{dj} = \mathbf{e}_{dj}^T \mathbf{P} \mathbf{e}_{dj}$ satisfies the conditions as required in Lemma 9.2 in [22] with constants c_1, c_2, c_3, c_4 given in terms of the eigenvalues of \mathbf{P} and \mathbf{Q} as: $c_1 = \lambda_{\min}(\mathbf{P})$, $c_2 = \lambda_{\max}(\mathbf{P})$, $c_3 = \lambda_{\min}(\mathbf{Q})$ and $c_4 = 2\lambda_{\max}(\mathbf{P})$. From Lemma 9.2 in [22], if $\|\mathbf{g}_{dj}\| \leq u_{ma} < \frac{c_3}{c_4} \sqrt{\frac{c_1}{c_2}} c_0 \bar{e}$ for all $t > 0$, all $\mathbf{e}_{dj} \in D = \{\mathbf{e}_{dj} \in \mathbb{R}^4 \mid \|\mathbf{e}_{dj}\| < \bar{e}\}$ with $c_0 < 1$, then for all $\|\mathbf{e}_{dj}(0)\| < \sqrt{\frac{c_1}{c_2}} \bar{e}$, the solution $\mathbf{e}_{dj}(t)$ of the perturbed system in (21) satisfies:

$$1) \frac{\|\mathbf{e}_{dj}(t)\|}{\|\mathbf{e}_{dj}(t_0)\|} \leq \sqrt{\frac{c_2}{c_1}} e^{(-\frac{(1-c_0)c_3}{2c_2})(t-t_0)}, \forall t_0 \leq t < t_0 + T_{dj},$$

$$2) \|\mathbf{e}_{dj}(t)\| \leq b_{dj} = \frac{c_4}{c_3} \sqrt{\frac{c_2}{c_1}} \frac{u_{ma}}{c_0}, \forall t \geq t_0 + T_{dj},$$

for some finite time T_{dj} . That is, \mathcal{D}_j tracks the desired trajectory $(\boldsymbol{\xi}_{dj}^s, \boldsymbol{\eta}_{dj}^s)$ within the error bound b_{dj} . Denote $b_d = \max_{j \in I_d} b_{dj}$. After the first two phases, all the defenders reach their desired locations within b_d neighborhood in finite time $T \geq T_d^g + \max_{j \in I_d} T_{dj}$ and hence the StringNet is formed in finite time. ■

¹Except for those in the set $\mathcal{M}_0 = \{\mathbf{r}_{dj}, \mathbf{v}_{dj} \in \mathbb{R}^2 \mid \forall j \in I_d \mid \mathbf{v}_{dj} = \mathbf{0}, \mathbf{u}_{dj} = \mathbf{0} \text{ as per (14), (17)}\}$, and the initial conditions from which the defenders' trajectories approach \mathcal{M}_0 ; the latter depends on the desired states. A formal characterization of this set is left open for future research.

Remark 2: All the attackers get entrapped inside the StringNet if the defenders form \mathcal{F}_d^g before the attackers reach within $\rho_{df}^g + \rho_{sn}$ distance from \mathcal{P} .

Theorem 2: Once the defenders form the StringNet \mathcal{G}^s , they herd all the attackers trapped inside \mathcal{G}^s to the safe area \mathcal{S} ($\rho_s > \rho_{sn}^{max}$) while avoiding the obstacles by tracking desired positions governed by (18) under the appropriately modified control action in (14).

Proof: Since the desired formation \mathcal{F}_d^h moves as a rigid formation, we only consider the virtual agent at \mathbf{r}_{df} with size $\rho_{sn} + \rho_d$ whose dynamics are:

$$\dot{\bar{\mathbf{r}}}_{df} = \mathbf{v}_{df}, \quad \dot{\mathbf{v}}_{df} = \boldsymbol{\sigma}_{dh}(\mathbf{u}_{df}^h) - C_d \mathbf{v}_{df}, \quad (22)$$

where $\mathbf{u}_{df}^h = -k_1 \bar{\mathbf{r}}_{df} + \sum_{k \in \mathcal{N}_{df}^o} \sigma_{df}^{\delta fk} \mathbf{u}_p(\mathbf{x}_{df}^{\delta fk})$ and $\bar{\mathbf{r}}_{df} = \mathbf{r}_{df} - \mathbf{r}_s$. Using similar arguments as in Theorem 1, we can ensure the safety of \mathcal{F}_d^h if $\hat{R}_{df}^{\delta ok} > \rho_{sn} + \rho_d + \bar{\rho}$, where $\bar{\rho} = \frac{u_{md}^h(1-\log(2))}{C_d^2}$ is the maximum distance the formation can travel in the worst case motion of the formation toward the obstacle with the bounded acceleration. The formation will leave the locally active potential fields around the static obstacle in some finite time. In the absence of any obstacle's local potential field, we have $\mathbf{u}_{df}^h = -k_1 \bar{\mathbf{r}}_{df}$. We define a candidate Lyapunov function:

$$V = \begin{cases} \frac{k_1 \|\bar{\mathbf{r}}_{df}\|^2}{2} + \frac{\|\mathbf{v}_{df}\|^2}{2}, & \text{if } \|\bar{\mathbf{r}}_{df}\| < \frac{u_{md}^h}{k_1}, \\ u_{md}^h \|\bar{\mathbf{r}}_{df}\| + \frac{\|\mathbf{v}_{df}\|^2}{2} - \frac{(u_{md}^h)^2}{2k_1}, & \text{otherwise.} \end{cases} \quad (23)$$

V is 0 at $\bar{\mathbf{r}}_{df} = \mathbf{v}_{df} = \mathbf{0}$, is positive definite, continuous and its time derivative along the trajectories of (22) is:

$$\dot{V} = \begin{cases} -C_d \|\mathbf{v}_{df}\|^2 & \text{if } \|\bar{\mathbf{r}}_{df}\| < \frac{u_{md}^h}{k_1}, \\ -C_d \|\mathbf{v}_{df}\|^2 & \text{otherwise.} \end{cases} \quad (24)$$

\dot{V} is negative semi-definite and we have from the dynamics (22) that the largest invariant subset in $\mathcal{Q} = \{\bar{\mathbf{r}}_{df}, \mathbf{v}_{df} \in \mathbb{R}^2 \mid \dot{V} = 0\}$ is the origin $\bar{\mathbf{r}}_{df} = \mathbf{v}_{df} = \mathbf{0}$. Using Lasalle's Invariance Principle (Theorem 4.4 in [22]), the trajectories of the system (22) converge to $\bar{\mathbf{r}}_{df} = \mathbf{v}_{df} = \mathbf{0}$, i.e., the center \mathbf{r}_{df} converges to \mathbf{r}_s and so does the desired formation \mathcal{F}_d^h . From Theorem 1, the defenders track these desired trajectories under appropriately modified (14) and hence herd the attackers to \mathcal{S} . ■

V. SIMULATIONS

We provide a simulation of 5 defenders herding an adversarial swarm of 4 attackers to \mathcal{S} with saturated control inputs whose theoretical analysis is currently an ongoing work. The trajectories of all the agents are shown in Fig. 3. As observed, starting from the given initial conditions, the defenders are able to gather before the attackers reach close to \mathcal{P} , form the StringNet around the attackers and herd them to \mathcal{S} . The safety is assessed in terms of critical distance ratios:

$$\Delta_d^d = \max_{j \neq j' \in I_d} \frac{\hat{R}_{dj}^{dj'}}{\hat{R}_{dj}^{dj}}, \Delta_a^d = \max_{i \in I_a, j \in I_d} \frac{\hat{R}_{dj}^{ai}}{\hat{R}_{dj}^{ai}}, \Delta_a^a = \max_{i \neq i' \in I_a} \frac{\hat{R}_{ai}^{ai'}}{\hat{R}_{ai}^{ai}}$$

$$\Delta_a^o = \max_{i \in I_a} \max_{k \in N_{ai}^o} \frac{\xi_{ok}^m}{E_{ok}^{ai}}, \quad \Delta_d^o = \max_{j \in I_d} \max_{k \in N_{dj}^o} \frac{\xi_{ok}^m}{E_{ok}^{dj}},$$

where E_{ok}^{ai}, E_{ok}^{dj} are super-elliptic distances from \mathcal{O}_k defined as per expression in (8). These ratios have to be less than 1 for no collisions. As observed from Fig. 4 all these ratios are less than 1 for all times ensuring no collisions.

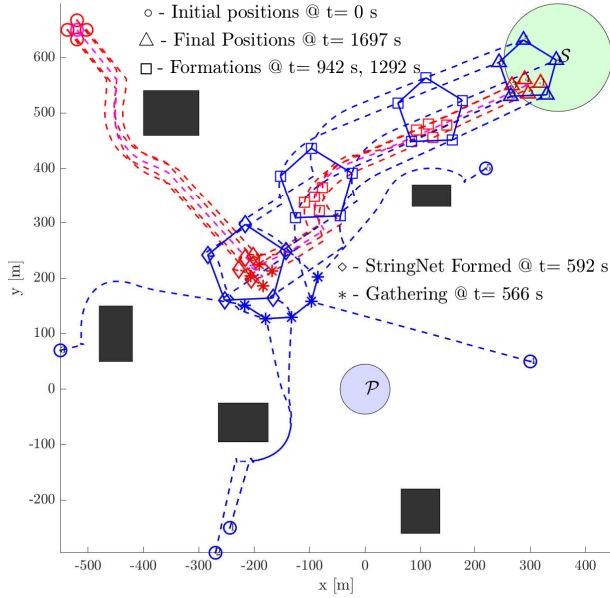


Fig. 3: The herding paths.

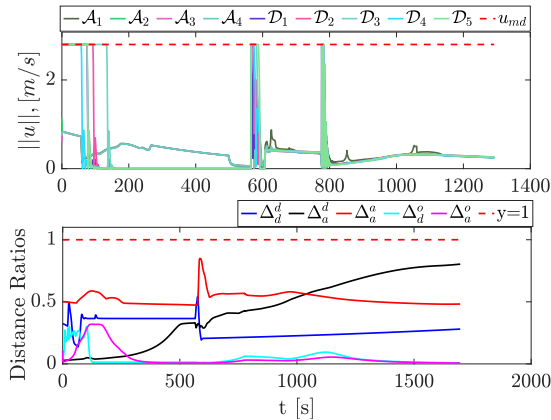


Fig. 4: Inputs and critical distances.

VI. CONCLUSIONS AND ONGOING WORK

We proposed a herding method for defending a protected area against an adversarial swarm. A closed formation is formed by the defenders around the attackers, restricts their motion and herds them to the safe area while avoiding the static rectangular obstacles. We provided formal analysis for the proposed approach and simulations with saturated control actions whose theoretical analysis and experimental investigation is a part of an ongoing work.

REFERENCES

[1] M. Chen, Z. Zhou, and C. J. Tomlin, "Multiplayer reach-avoid games via pairwise outcomes," *IEEE Transactions on Automatic Control*, vol. 62, no. 3, pp. 1451–1457, 2017.

[2] M. Coon and D. Panagou, "Control strategies for multiplayer target-attacker-defender differential games with double integrator dynamics," in *Conference on Decision and Control*. IEEE, 2017, pp. 1496–1502.

[3] S. Gade, A. A. Paranjape, and S.-J. Chung, "Herding a flock of birds approaching an airport using an unmanned aerial vehicle," in *AIAA Guidance, Navigation, and Control Conference*, 2015, p. 1540.

[4] —, "Robotic herding using wavefront algorithm: Performance and stability," in *AIAA Guidance, Navigation, and Control Conference*, 2016, p. 1378.

[5] A. A. Paranjape, S.-J. Chung, K. Kim, and D. H. Shim, "Robotic herding of a flock of birds using an unmanned aerial vehicle," *IEEE Transactions on Robotics*, vol. 34, no. 4, pp. 901–915, 2018.

[6] A. Pierson and M. Schwager, "Controlling noncooperative herds with robotic herders," *IEEE Transactions on Robotics*, vol. 34, no. 2, pp. 517–525, 2018.

[7] M. A. Haque, A. R. Rahmani, and M. B. Egerstedt, "Biologically inspired confinement of multi-robot systems," *International Journal of Bio-Inspired Computation*, vol. 3, no. 4, pp. 213–224, 2011.

[8] A. Varava, K. Hang, D. Kragic, and F. T. Pokorný, "Herding by caging: a topological approach towards guiding moving agents via mobile robots," in *Proceedings of Robotics: Science and Systems*, 2017.

[9] R. A. Licitra, Z. D. Hutcheson, E. A. Doucette, and W. E. Dixon, "Single agent herding of n-agents: A switched systems approach," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 14374–14379, 2017.

[10] R. A. Licitra, Z. I. Bell, E. A. Doucette, and W. E. Dixon, "Single agent indirect herding of multiple targets: A switched adaptive control approach," *IEEE Control Systems Letters*, vol. 2, no. 1, pp. 127–132, 2018.

[11] P. Deptula, Z. I. Bell, F. M. Zegers, R. A. Licitra, and W. E. Dixon, "Single agent indirect herding via approximate dynamic programming," in *2018 IEEE Conference on Decision and Control (CDC)*. IEEE, 2018, pp. 7136–7141.

[12] V. S. Chipade and D. Panagou, "Herding an adversarial attacker to a safe area for defending safety-critical infrastructure," *arXiv preprint arXiv:1903.06365*, 2019.

[13] C. W. Reynolds, "Flocks, herds and schools: A distributed behavioral model," in *ACM SIGGRAPH computer graphics*, vol. 21, no. 4. ACM, 1987, pp. 25–34.

[14] R. O. S. R. Murray and R. Saber, "Flocking with obstacle avoidance: Cooperation with limited information in mobile networks," in *Proceedings of the 42nd IEEE Conference on Decision and Control*, vol. 2. Citeseer, 2003, pp. 2022–2028.

[15] R. Olfati-Saber, "Flocking for multi-agent dynamic systems: Algorithms and theory," California Inst of Tech Pasadena Control and Dynamical Systems, Tech. Rep., 2004.

[16] B. Dai and W. Li, "Flocking of multi-agents with arbitrary shape obstacle," in *Proceedings of the 33rd Chinese Control Conference*. IEEE, 2014, pp. 1311–1316.

[17] H. G. Tanner, A. Jadbabaie, and G. J. Pappas, "Flocking in fixed and switching networks," *IEEE Transactions on Automatic control*, vol. 52, no. 5, pp. 863–868, 2007.

[18] D. Panagou, "Motion planning and collision avoidance using navigation vector fields," in *Proc. of the Int. Conf. on Robotics and Automation*. IEEE, 2014, pp. 2513–2518.

[19] M. Deghat, B. D. Anderson, and Z. Lin, "Combined flocking and distance-based shape control of multi-agent formations," *IEEE Transactions on Automatic Control*, vol. 61, no. 7, pp. 1824–1837, 2016.

[20] R. Volpe and P. Khosla, "Manipulator control with superquadric artificial potential functions: Theory and experiments," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 20, no. 6, pp. 1423–1436, 1990.

[21] S. P. Bhat and D. S. Bernstein, "Geometric homogeneity with applications to finite-time stability," *Mathematics of Control, Signals and Systems*, vol. 17, no. 2, pp. 101–127, 2005.

[22] H. K. Khalil, *Nonlinear control*. Pearson New York, 2015.