Hindawi
Security and Communication Networks
Volume 2020, Article ID 8889122, 15 pages
https://doi.org/10.1155/2020/8889122

Research Article

Exposing Spoofing Attack on Flocking-Based Unmanned Aerial Vehicle Cluster: A Threat to Swarm Intelligence

Xinyu Huang[1], **Yunzhe Tian**[1], **Yifei He**[1], **Endong Tong**[1], **Wenjia Niu**[1], **Chenyang Li**[1], **Jiqiang Liu**[1] and **Liang Chang**[2]

[1]*Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, 3 Shangyuan Village, Haidian District, Beijing 100044, China*
[2]*Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541004, China*

Correspondence should be addressed to Endong Tong; edtong@bjtu.edu.cn and Wenjia Niu; niuwj@bjtu.edu.cn

Received 10 August 2020; Revised 4 November 2020; Accepted 29 November 2020; Published 10 December 2020

Academic Editor: Zhihua Xia

With the rapid development of wireless communication technology and intelligent mobile devices, unmanned aerial vehicle (UAV) cluster is becoming increasingly popular in both civilian and military applications. Recently, a swarm intelligence-based UAV cluster study, aiming to enable efficient and autonomous collaboration, has drawn lots of interest. However, new security problems may be introduced with such swarm intelligence. In this work, we perform the first detailed security analysis to a kind of flocking-based UAV cluster with 5 policies, an upgrade version of the well-known Boids model. Targeting a realistic threat in a source-to-destination flying task, we design a data spoofing strategy and further perform complete vulnerability analysis. We reveal that such design and implementation are highly vulnerable. After breaking through the authentication of ad hoc on-demand distance vector (AODV) routing protocol by rushing attack, an attacker can masquerade as the first-arrival UAV within a specific scope of destination and generate data spoofing of arrival status to the following UAVs, so as to interfere with their normal flying paths of destination arrival and cause unexpected arrival delays amid urgent tasks. Experiments with detailed analysis from the 5-UAV cluster to the 10-UAV cluster are conducted to show specific feature composition-based attack effect and corresponding average delay. We also discuss promising defense suggestions leveraging the insights from our analysis.

1. Introduction

UAVs have been widely used in military and civilian fields due to their low cost and high flexibility. With the rapid development of wireless communication technology and mobile devices, the unmanned aerial vehicle cluster is becoming increasingly popular in tasks of monitoring, search, and rescue in a dangerous environment. Recently, swarm intelligence in the field of AI has been employed in the UAV cluster to provide an efficient and effective collaboration of UAVs that does not require any external remote guidance or any central-node UAV control, amid complex tasks difficult for a single UAV. Thus, the multi-UAV cluster aims to realize an autonomous mechanism by imitating different kinds of swarm including a flock of birds and a swarm of bees. Although such swarm intelligence has shown its potential to provide an efficient and effective UAV collaboration, few studies focus on the security issues brought by swarm intelligence. Thus, it is highly important to deep assess the security of swarm intelligence-based UAV cluster and discover a possible vulnerability that can be maliciously exploited.

In this paper, we focus on the swarm intelligence of flocking inspired by birds. There is a classical model named Boids model [1] proposed by Reynolds in 1986, of which there is no central node and each UAV is autonomous through perceiving its neighbors' information within a certain range nearby [2, 3]. Each UAV's decision-making is based on three simple policies: dispersion, alignment, and cohesion. Such a collaboration mechanism of policies derives from the birds' flocking; thus, it is also called flocking in short. In this work, we choose the latest upgraded version of

the Boids model including five policies: alignment, homing, cohesion, dispersion, and following, which is more complete for flocking [4]. In the rest of this paper, the flocking is always referred to as this 5-policy flocking. Also, we target a source-to-destination flying task for cluster flying and perform the first detailed security analysis to the flocking-based UAV cluster flying. To the best of our knowledge, no similar work has focused on it.

Facing cyberattacks, it is highly important to firstly understand potential security vulnerabilities so that they can be actively resolved before real large-scale deployment. As the first step, we implement the 5-policy flocking algorithm. Through tuning a set of parameters, we successfully realize the flocking to maintain a relatively stable formation for UAV cluster flying. Then we identify basic security challenges, involved authentication, data spoofing, and so on, aiming to understand whether the current design or implementation of the flocking algorithm for UAV cluster is vulnerable and why it is vulnerable and hope to provide insights on how to fundamentally protect it before large-scale UAV cluster deployment.

For simplicity, we assume that the UAVs in the cluster move at a constant speed and use the mobile ad hoc network (MANET) [5] to exchange data with other UAVs within the specific range of wireless sensing. The data includes GPS location, speed direction, and arrival status. The only attack requirement that we limit is that there is just one UAV masqueraded to send spoofed data to other UAVs. This can be realized by a rushing attack to break through the authentication of the ad hoc on-demand distance vector (AODV) routing protocol [6, 7]. As reported in former work, such compromise can be performed physically [8], wirelessly [9], or through malware [10, 11]. Thus, only rushing attack one first-arrival UAV for data spoofing of arrival status is closer to the attack reality and ensures that our analysis has highly practical implications.

In this work, we find that data spoofing of arrival status is very effective for autonomous flocking-based UAV cluster: through masqueraded UAV sending spoofed data to the following UAVs, the maximum percentage of delay can even reach up to nearly 50%, which completely subverts the advantage of the flocking, as a highly efficient algorithm. Figure 1 shows an attack snapshot of the simulation for 8-UAV flocking-based flying from the left sources to the right destinations (denoted as red circles, respectively) in farmland. The axes represent the flying coordinates in meters. Figure 1(a)) shows the attack place occurring to the first-arrival UAV. As shown in Figure 1(b)), during the attack, some UAVs' trajectories in the cluster have been affected (seen in the green circle) and caused an obvious delay to their destinations. We find that this is due to a vulnerability in the trade-off between security and formation stability: in the flocking algorithm, to maintain the stability of the cluster formation, once a UAV has reached its destination, its information will not be used in the other UAVs' decision-making anymore.

In our experiment, we find the following: (1) fixing the arrival determining threshold with 20 meters, the delay percentage of smaller UAV cluster is higher than that of a larger cluster, which appears from cluster speed 10 m/s to 20 m/s; (2) lower arrival determining threshold will cause an opposite result, that is, larger cluster having higher delay percentage; (3) fixing the cluster's speed, whatever the cluster size is, lower arrival determining threshold will cause a higher delay percentage; (4) the maximum delay percentage of 47.84% is obtained in the occasion of cluster size 9, cluster speed 16 m/s, and arrival determining threshold 12 meters.

According to our analysis, the current flocking algorithm design is highly vulnerable to data spoofing, causing the whole UAV cluster to delay its arrival to a large extent. We also discuss promising defense directions leveraging the insights from our analysis.

We summarize our contributions as follows:

(i) We perform the first security analysis of flocking-based UAV cluster flying. We formulate the problem with a highly realistic threat model, involved AODV link authentication, rushing attack, and data spoofing to UAV cluster and analyze the algorithm design to identify the data spoofing strategy.

(ii) Targeting the goal of causing unexpected arrival delays in flying task, we first perform vulnerability analysis to understand the attack effectiveness. We find that the flocking algorithm design and implementation are highly vulnerable, causing nearly 50% arrival delay in some cases.

(iii) Through massive experiments, we obtain detailed attack results under different cluster features, which helps to provide promising defense directions from our analysis and experimental results.

2. Background

In this section, we introduce the necessary background about the swarm intelligence in the UAV cluster and the flocking algorithm that we target.

2.1. UAV Swarm Intelligence. Swarming behavior is a common phenomenon in nature. Typical examples include flocks of birds migrating in formation, schools of fish parading in groups, colonies of ants working together, and colonies of bacteria that grow together. The common feature of these phenomena is that a certain number of autonomous individuals, through mutual collaboration and self-organization, present an orderly coordinated movement and behavior on the collective level [12]. In the early stage of research in this area, a lot of work focused on modeling and simulation of natural biological populations. Scholars use a large amount of experimental data to explore the influence of individual behavior and the relationship between individuals on the overall behavior of the group [13, 14].

In the field of UAV, the Boids model is naturally applied as the earliest swarm intelligence model, establishing and maintaining collision-free cohesive flocking which requires only three simple policies between idealistic agents: (1)

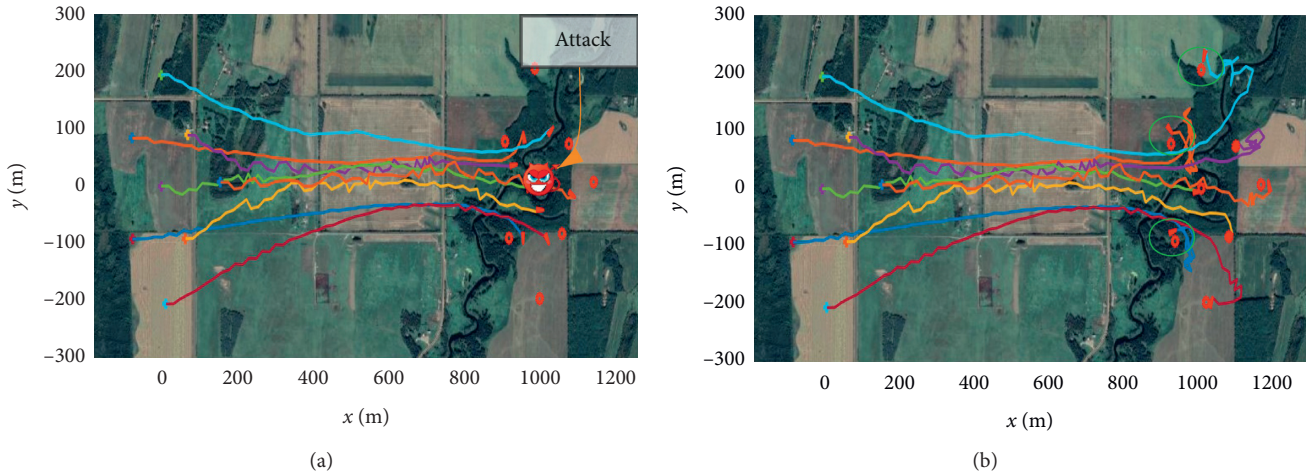

Figure 1: A snapshot of the simulation of 8-UAV flocking-based cluster flying. (a) The attack place to first-arrival UAV. (b) Arrival delays with affected trajectories in green circles.

gathering: make the agents in the entire group closely adjacent; (2) keeping distance: adjacent agents keep a safe distance; (3) motion matching: neighboring agents have the same motion state. This model roughly describes the movement characteristics of swarms in nature. Lately, Sharma and Ghose extended the Boids and proposed a swarm intelligence algorithm to avoid cluster collisions [4]. Our work is based on Sharma et al.'s algorithm to build a flocking-based UAV cluster as our target of security analysis.

2.2. Flocking Algorithm. In a UAV cluster, the equation of motion in the two-dimensional plane for a UAV can be represented as

$$\begin{cases} \dot{x}_i = \mathbf{v}\cos\theta_i, \\ \dot{y}_i = \mathbf{v}\sin\theta_i, \\ \dot{\theta}_i = \dfrac{\eta}{V}, \end{cases} \tag{1}$$

where $\mathbf{x}_i$, $\mathbf{y}_i$, θ_i are the x-axis coordinate, y-axis coordinate, and heading angle of the i-th UAV, respectively. $V = |\mathbf{v}|$ means UAV's speed and η is the acceleration. The detailed calculation is shown as follows:

$$\begin{aligned} \eta &= k\Delta\theta_i, \\ \Delta\theta_i &= w_1\left(\theta_{\text{req1}} - \theta_i\right) + w_2\left(\theta_{\text{req2}} - \theta_i\right) + \cdots + w_n\left(\theta_{\text{req}\,m} - \theta_i\right), \end{aligned} \tag{2}$$

where k is the acceleration constant and $\theta_{\text{req1}}, \theta_{\text{req2}}, \ldots, \theta_{\text{req}\,m}$ are the desired heading angles corresponding to different policies. We can vary the policy weights $w_1, w_2, \ldots, w_m$ to obtain different composite policies.

We target the flocking with five basic policies including cohesion, dispersion, following, homing, and alignment as shown in Table 1.

We use w_h, w_a, w_c, w_d, w_f to represent the weight of homing, alignment, cohesion, dispersion, and following policies, respectively.

Figure 2 shows the heading angle computation of a UAV in the cluster. The above basic policies can ensure that the self-organized UAV swarm remains stable and collision-free during the flight. However, when the UAV swarm arrives near the destination, if the arrived UAV is still involved in the angle calculations for other unreached UAVs, the directions of the unreached UAVs will be affected not to reach their destinations. Thus, once there is a UAV in the cluster that has reached its destination, it has to be timely excluded from the calculations.

Also, in general, to determine whether a UAV has arrived, we calculate the distance between the current location of the UAV and the destination, in which the specified parameter R is defined as an arrival determining the threshold. When the distance between the current location of the UAV and the destination is less than R, the UAV is determined to have reached its destination.

3. Threat Model

3.1. Communication. In the UAV cluster, MANET is a common-used communication network to support UAVs' communication (see Figure 3) [15]. There are two channels: data channel and protocol channel. In our experiment, we limit three data to transmit including heading angle, coordinate, and arrival status.

As we can see, MANET is an ad hoc decentralized type of wireless network that does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks [5]. Instead, each node participates in routing by forwarding data to other nodes, so the determination of which nodes forward data is made dynamically based on network connectivity and the routing algorithm in use [16]. Such wireless networks lack the complexities of infrastructure setup and administration

Table 1: Desired heading angles based on different policies in the flocking algorithm.

Policies	Desired heading angles	Notation
Cohesion	$\theta_{Ci} = \arctan((Y_{C_{\rho,i}} - y_i)/(X_{C_{\rho,i}} - x_i))$	$(X_{C_{\rho,i}}, Y_{C_{\rho,i}})$: the centroid of all UAVs in sensor range ρ
Dispersion	$\theta_{Di} = \arctan((y_i - Y_{C_{d,i}})/(X_{C_{d,i}} - x_i))$	$(X_{C_{d,i}}, Y_{C_{d,i}})$: the centroid of all UAVs within the $d_{\min}$ range
Following	$\theta_{Fi} = (\theta_{Ni} + \theta_{Ri})/2$ $\theta_{Ri} = \arctan((Y_{Ri} - y_i)/(X_{Ri} - x_i))$ $\theta_{Ni} = \arctan((Y_{Ni} - y_i)/(X_{Ni} - x_i))$	(X_{Ri}, Y_{Ri}): the coordinate of the randomly selected UAV (X_{Ni}, Y_{Ni}): the coordinate of the nearest UAV
Homing	$\theta_{Hi} = \arctan((Y_{Hi} - y_i)/(X_{Hi} - x_i))$	(X_{Hi}, Y_{Hi}): the destination coordinate
Alignment	$\theta_{Ai} = (1/n_i)\sum_{j=1}^{n_i} \theta_j$	θ_j: the heading angle of j-th UAV
Combined	$\theta_i' = \theta_i + \Delta\theta_i$ $\Delta\theta_i = w_h(\theta_{Hi} - \theta_i) + w_a(\theta_{Ai} - \theta_i) + w_c(\theta_{Ci} - \theta_i) + w_d(\theta_{Di} - \theta_i) + w_f(\theta_{Fi} - \theta_i)$	w_h, w_a, w_c, w_d, w_f: weights

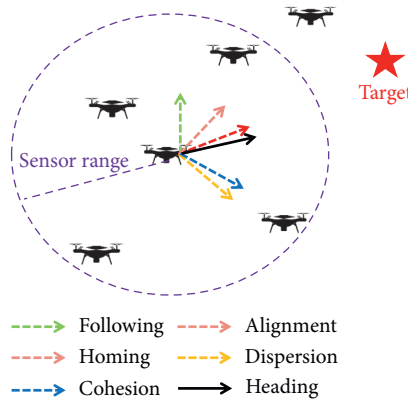

Figure 2: The heading angle of a UAV in its sensor range. By combining the 5 policies' weight, the heading angle is calculated according to vector addition.

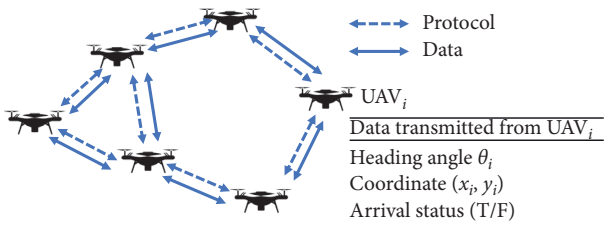

Figure 3: The MANET-based UAV communication. The transmitted data is limited to the heading angle, coordinate, and arrival status.

while enabling UAVs to create and join networks anytime efficiently.

Due to common attacks in MANET, there is also a communication-related threat to the flocking-based cluster [17], such as wormhole attack, rushing attack, joint attack, Sybil attack, denial of service attacks, and eavesdropping attacks. In this work, we only utilize one communication attack: the rushing attack.

Through the rushing attack, data spoofing can be performed. Previous work has demonstrated sensor spoofing attacks to single UAV, such as GPS spoofing [18, 19] to misguide UAV's trajectory and optical spoofing [20, 21] to gain an implicit control channel. Thus, it is confident to assume that the attacker can perform data spoofing in any type, physically [8], wirelessly [9], or through malware [10, 11].

3.2. AODV Link Authentication. MANET is inherently vulnerable to attack due to its fundamental characteristics, such as open medium, distributed nodes, the autonomy of nodes participation in a network (nodes can join and leave the network on its will), lack of centralized authority which can enforce security on the network, distributed coordination, and cooperation [6].

Many of the routing protocols devised for use in MANET have their individual character and rules. The most widely used routing protocol is AODV, which relies on the individual node's cooperation in establishing a valid routing table. However, it only enables a weak link authentication based on all nodes trusted in the network. In the AODV protocol, each node first establishes a valid route to the destination before transmitting its data. Sender node broadcasts an RREQ (route request) message to neighbors and valid route replies with RREP (route reply) with proper route information. The AODV protocol uses a duplicate suppression mechanism to limit the route request and reply chatter in the network (see Figure 4). In Figure 4(a)), there are three RREQ messages.

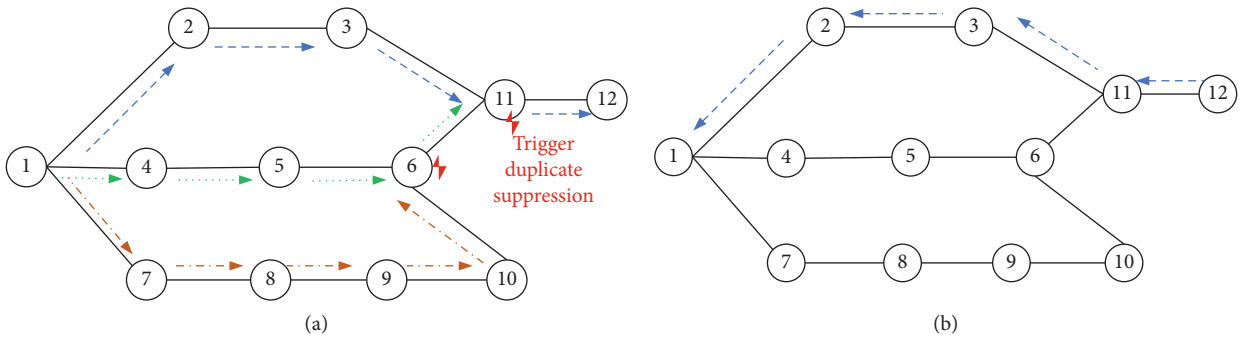

FIGURE 4: The duplicate suppression mechanism in AODV protocol, only with a weak link authentication. (a) RREQ process. (b) RREP process.

Due to the first arrival of the blue path, the duplicate suppression is triggered to ensure that the blue path is a valid link-authenticated one as the right subfigure shows.

Although AODV has high efficiency and complexity, AODV does not have heavy node authentication. Thus, once a malicious node can join and disrupt the network by hijacking the routing tables or bypassing valid routes, then it has a chance to eavesdrop on the network if the node can establish the shortest route to any destination by exploiting the unsecured routing protocols [6].

As shown in Figure 5, the attacker joins the network easily using a rushing attack. The attacker quickly forwards a malicious RREP. Due to duplicate suppression, an actual valid RREP message from the valid node will be discarded and consequently, the attacking node becomes part of the route. After that, the attacker can change the data from the initiator node. To maximize the realism of our threat model, in this paper we assume that only one heading UAV is attacked.

4. Attack Construction

In this section, we describe the attack goal and present the data spoofing attack to affect the flocking.

4.1. Attack Goal: Arrival Delay. As the first security study on the flocking-based UAV cluster, our analysis in this paper focuses on interfering with the UAV cluster's normal flying paths to the destination, causing unexpected delays. More specifically, the attacker aims to pretend to be the first arrived UAV to further send spoofed data to the following UAVs and interferes with their heading angles (see Figure 6).

Such an attack can cause economic losses and affect production work. For example, one of the most potential applications of UAV cluster is for monitoring, search, and rescue in a dangerous environment. Using UAVs to do such a task can reduce unnecessary casualties, and thus, it is highly important to ensure that such flying is well protected and functions correctly and efficiently. Of course, the attacker can also attack multiple heading UAVs at the same time.

4.2. Security Analysis and Attack Flow. Our security analysis consists of the following key steps:

(1) Data spoofing strategy identification: before analyzing the vulnerability of the flocking algorithm, we first need to identify meaningful data spoofing strategies. We analyze the parameter data flow to understand how the spoofed data can potentially influence the UAV cluster.

(2) Vulnerability analysis: with the data spoofing strategy identified, we then further perform vulnerability analysis to reveal the attack consequences. To ensure the generality of this analysis, we choose the most potential application of UAV cluster in flying tasks for monitoring, search, and rescue in a dangerous environment and compare the flying trajectory and total time of the task with and without attack.

(3) Cause analysis and exploit construction: with the attack effectiveness for data spoofing quantified, we perform cause analysis for the successful attacks to understand why the current flocking algorithm is vulnerable. Leveraging the insights, we construct corresponding exploits.

Figure 7 shows the attacked data flow. An attacker can masquerade as the first-arrival UAV within a specific scope of destination and generate data spoofing of arrival status to the following UAVs. Note that GPS and gyroscope are not spoofed. Due to the affected heading angle computed based on weights set of policies, the attacker can interfere with normal flying paths of destination arrival, causing unexpected arrival delays.

The detailed data spoofing attack process is shown in Algorithm 1.

5. Attack Evaluation

5.1. Setup. We perform a real-world source-to-destination flying task in a simulation environment. The swarm consists of five to ten UAVs and uses the flocking algorithm. This

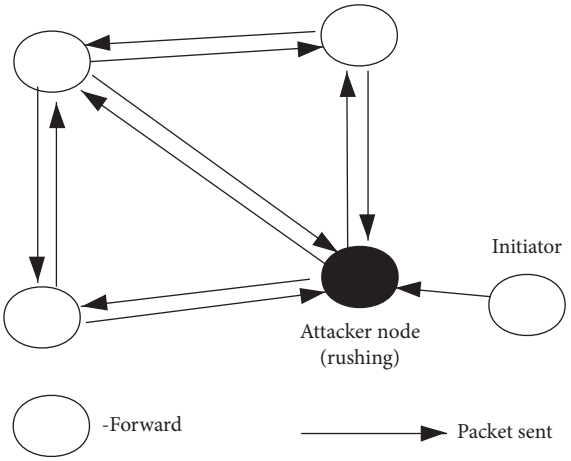

Figure 5: Rushing attack launched by the attacker node.

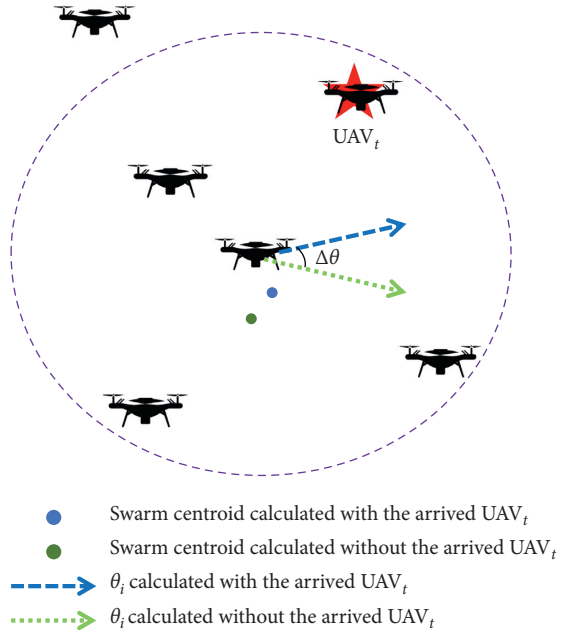

Figure 6: The illustration of attack for interfering heading angle by comparing different centroids.

paper uses a laptop computer as the simulation experiment platform to match the real attack scene, and the software platform is MATLAB R2019b. The experimental environment configuration is shown in Table 2.

5.2. Feature Computation. We hope to bring a delay of the UAV swarm arriving at the target points. When the cluster is about to reach the target, we launch a rushing attack to the arrived UAV in the MANET, by changing the arrival status data from T (arrived) to F (not arrived), and send the arrival status data to other UAVs. In this way, the following UAVs will calculate to get a wrong heading angle which will increase the length of their trajectories to the target points and cause arrival delay. In the analysis, we use the increased delay time under attack as a percentage of the original time of the flying task to quantify the effectiveness of our attack.

5.3. Influence from Speed. We first evaluate the impact of UAV speed on our attack. We take six different UAV speeds from 10 m/s to 20 m/s to study the effect of speed changes on the delay under a fixed arrival determining threshold $R = 20$ m. In order to have universal applicability, we conduct experiments in the case of 5–10 UAV clusters. In the experiments, the initial coordinates of UAVs are random points within five to ten ranges (to ensure the initial safety distance). The target points are 1000 m away from the initial coordinates and the structure of target points is consistent with the initial points' structure. The velocity of UAVs is

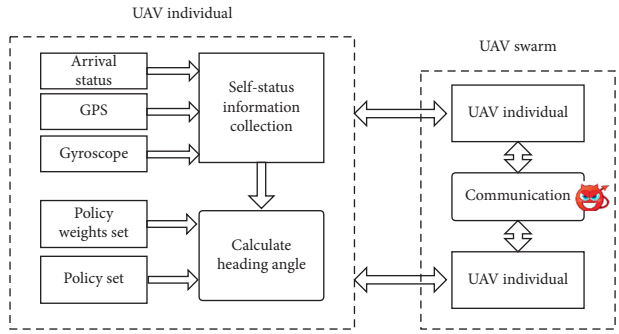

Figure 7: The attacked data flow in the UAV swarm.

Input: R (arrival determining threshold), UAV_i(i-th UAV)
Output: $\theta_i^{,\text{attack}}$ (desired combined heading angle of the i-th UAV after the attack)
(1) *//normal*
(2) **when** the first-arrival UAV_t is within R scope of its destination **then**:
(3) UAV_t sends arrival status (T) to the following UAVs;
(4) UAV_i flies along its desired combined heading angle θ_i' calculated by flocking algorithm without UAV_t;
(5) *//with attack*
(6) **when** the first-arrival UAV_t is within R scope of its destination **then**:
(7) Attacker masquerades as UAV_t exploiting rushing attack;
(8) The attacker generates data spoofing of arrival status and sends the malicious arrival status (F) to following UAVs;
(9) UAV_i flies along its desired combined heading angle $\theta_i^{',\text{attack}}$ calculated by flocking algorithm including UAV_t;
(10) **return** $\theta_i^{',\text{attack}}$

Algorithm 1: Data spoofing attack algorithm.

Table 2: Experimental environment configuration.

Experimental environment	Environmental configuration
Operating system	macOS
CPU	2.4 GHz Intel Core i5
Memory	16 GB
Hardware	500 G
Main tools	MATLAB R2019b

from $V = 10$ m/s to $V = 20$ m/s, the maximum communication range among UAVs is $\rho = 150$ m, the threshold for the application of the cohesion policy is $d_{\max} = 120$ m, and the threshold for the application of the dispersion policy is $d_{\min} = 30$ m. The threshold for judging whether the UAV has reached the target point is $R = 20$ m; that is, when the distance between the location of the UAV and its target point is less than 20 m, it can be regarded as having arrived. The weight of 5 policies is $w_h = 0.9, w_a = 0.5, w_c = 0.2, w_d = 0.4$, and $w_f = 0.1$. This set of weights can ensure that the UAV cluster can fly smoothly to the destination when it is not attacked.

The experiment results are shown in Figure 8. Figures 8(a)–8(f)) are corresponding to different UAV numbers of the cluster from 5 to 10. We can see that the medium numbers in each experiment are over 10% and tend to increase first and then decrease with the speed of the cluster. The corresponding average percentage of delays increment is summarized in Table 3. We use the increased delay time as a percentage of the original time of the task to quantify the effectiveness of our attack. In these columns, each value is the average delay increment under attack as a percentage of the average task completion time without attack.

In this experiment, we fix the arrival determining the threshold at 20 meters. We find the following: (1) from the general trend, the delay increment percentage of a smaller UAV cluster is higher than that of a larger cluster; (2) for a given cluster size, the average percentage of delay increment first increases with cluster speed and then decreases; (3) the maximum delay increment percentage of 27.76% is obtained in the occasion of cluster size 8 and cluster speed 16 m/s.

5.4. Influence from Threshold R. Then, we evaluate the impact of arrival determining threshold R on our attack. We took five different arrival determining threshold from 12 m to 20 m for experiments to study the effect of arrival determining threshold R on the delay under different UAV speeds. In order to have universal applicability, we conducted experiments in the case of 5–10 UAV clusters. In the experiment, the initial coordinates of UAVs are random points within five to ten ranges (to ensure the initial safety distance). The target points are 1000 m away from the initial coordinates and the structure of target points is consistent with the initial points' structure. The velocity of UAVs is from $V = 10$ m/s to $V = 20$ m/s, the maximum communication range between UAVs is $\rho = 150$ m, the threshold for

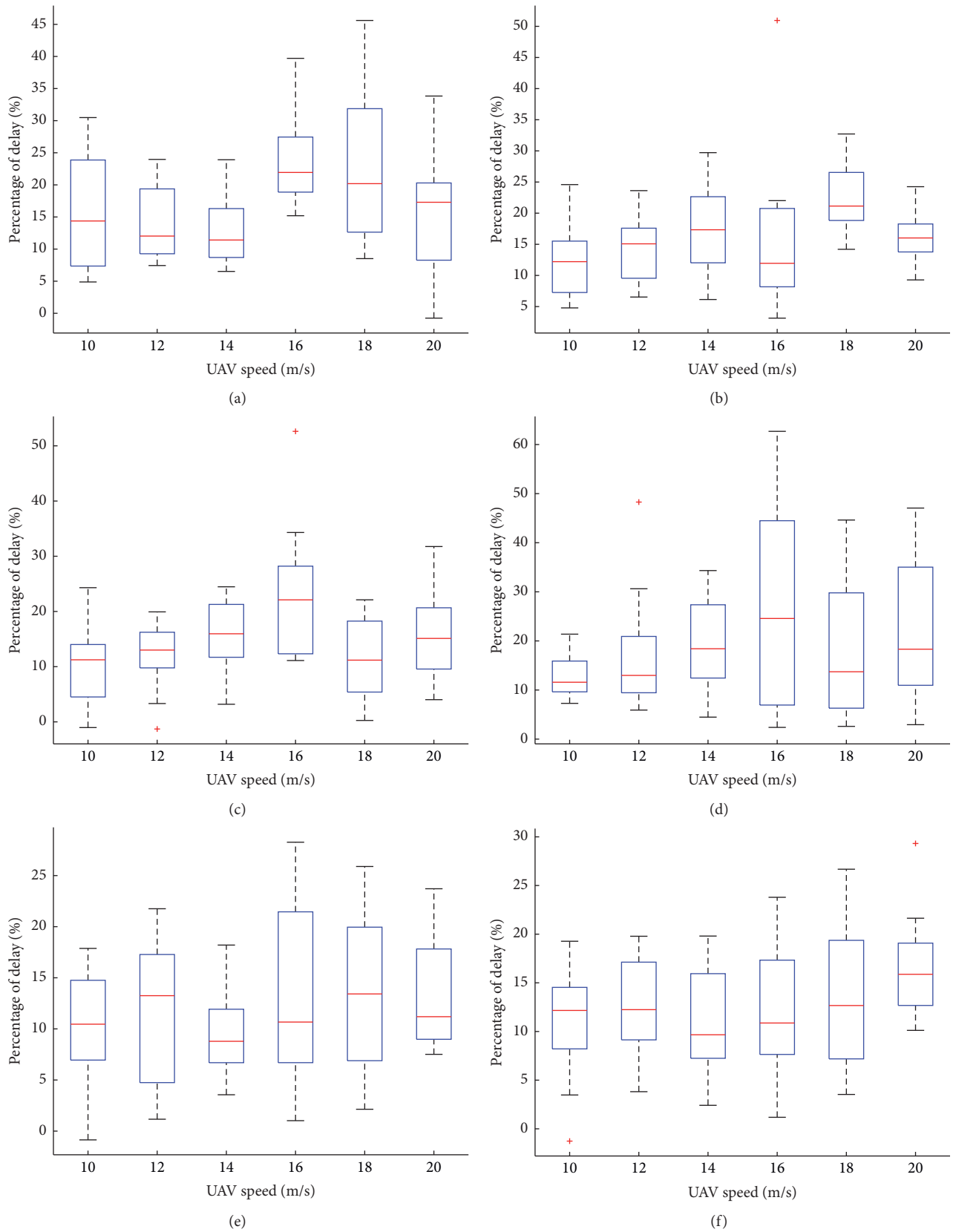

FIGURE 8: Delay increment for multi-UAV clusters of different sizes at a speed from 10 to 20 m/s and with $R = 20$. (a) Boxplot for 5-UAV clusters. (b) Boxplot for 6-UAV clusters. (c) Boxplot for 7-UAV clusters. (d) Boxplot for 8-UAV clusters. (e) Boxplot for 9-UAV clusters. (f) Boxplot for 10-UAV clusters.

Table 3: Average delay increment comparison with $R = 20$.

Speed (m/s)	5-UAV cluster (%)	6-UAV cluster (%)	7-UAV cluster (%)	8-UAV cluster (%)	9-UAV cluster (%)	10-UAV cluster (%)
10	15.70	12.79	10.37	13.08	9.76	10.90
12	13.77	14.47	11.72	17.74	11.55	12.42
14	12.83	17.33	15.53	19.10	9.52	11.01
16	25.00	15.97	23.69	**27.76**	12.83	11.52
18	22.39	22.22	11.17	18.29	13.66	13.76
20	15.64	16.17	15.67	21.66	13.70	17.03

the application of the cohesion policy is $d_{\max} = 120$ m, and the threshold for the application of the dispersion policy is $d_{\min} = 30$ m. The arrival determining threshold R is between 12 m and 20 m. The weight of 5 policies is $w_h = 0.9, w_a = 0.5, w_c = 0.2, w_d = 0.4$, and $w_f = 0.1$.

The experiment results are shown in Figure 9. The corresponding average percentage of delays increment is summarized in Tables 4–9. In this experiment, we find that when fixing the cluster's speed, lower arrival determining threshold R will cause a higher delay increment percentage no matter what the cluster size; the maximum delay increment percentage of 47.84% is obtained in the occasion of cluster size 9, cluster speed 16 m/s, and arrival determining threshold 12 meters.

6. Defense Suggestion

As our research shows, even though the swarm intelligence algorithm shows high effectiveness under a benign set of weights, the current algorithm design is still very vulnerable to data spoofing attacks. In order to proactively solve these problems before large-scale deployment, this section discusses the defense direction based on the insights derived from our analysis.

From our experimental analysis, compared with the higher arrival determining threshold R, a lower R will cause a higher delay percentage because it is difficult to fly very close to the destination especially at a highly fast speed and under the data spoofing attack. Thus, we suggest increasing R in a reasonable practical range to match the speed. But it is a trade-off between accuracy and safety because if we use a too high value of R, the cluster will lose its accuracy and stop too far away from the destination.

Similarly, UAVs at a constant higher speed will not steadily fly to the destination when it approaches the destination and under the attack. To ensure the efficiency of performing tasks, the speed setting can be divided into two stages. In the beginning, UAVs fly at a higher speed. When they approach their destinations, a lower speed should be adopted for a steady fly towards the destination.

Another possible defense is increasing the weight of homing policy and decreasing the weight of cohesion, following, and alignment policies especially when the swarm approaches the destination. In this case, although the first-arrival UAV is attacked, the following UAVs will still fly towards their destination due to the enhanced homing force and thus can decrease the influence of attack. Thus, it is highly important to adjust policy weights and speed dynamically and timely according to the current state to achieve a robust, conflict-free, and efficient UAV swarm.

The data spoofing attack against UAV clusters is rooted from the attacker breaking through the vulnerable authentication of AODV exploiting a rushing attack. Several robust defenses against rushing attack can be introduced in the multi-UAV cluster communication network [7], such as secure neighbor detection which allowed the sender and the receiver to verify that the other party is within the normal direct wireless communication range because the attacker often forwards an RREQ beyond the normal radio transmission range to achieve faster transit; randomized RREQ forwarding allowed a node first to collect a number of RREQs and select one at random to forward to replace traditional duplicate suppression mechanism in AODV which could be exploited by rushing attackers and blacklist mechanisms using the property of nonrepudiation to spread information about identified malicious nodes. Also, there is always a trade-off issue between strong authentication and flocking efficiency, requiring further light authentication study.

7. Related Works

7.1. Data Spoofing in UAV. In [8, 9], the authors demonstrated the feasibility of infiltrating internal networks to launch data spoofing through the network node. Lately, a lot of studies show the sensor's attack to launch data spoofing. More specifically, the GPS spoofing [18, 22] by sending interfering signals is very common. In addition to GPS sensors, other sensors including optical sensors [20, 21] and context-aware services [23–26] can also be threatened to cause data spoofing physically [8, 19, 20, 27–29], wirelessly [9, 30, 31], or through malware [10, 11]. Similar to previous work, our data spoofing is launched through a node in the ad hoc network. Some attacks have been revealed involving wormhole attack, rushing attack, joint attack, Sybil attack, denial of service attacks, and eavesdropping attacks [17]. Prior to our work, there are some related works to attack UAV. The detailed comparison is given in Table 10. We can see that our work focuses on attacking the swarm algorithm as our directed target, compared to those physical sensors or software modules. In addition, compared to the Partial Differential Equation (PDE) algorithm [31], the flocking algorithm enables more control policy that is more practical in real applications. As to the attack effect, general effects include position error, crash, unstable flight, path deviation, and time delay. Although without a crash, our method discovers the attack to cause a heavy time delay of swarm

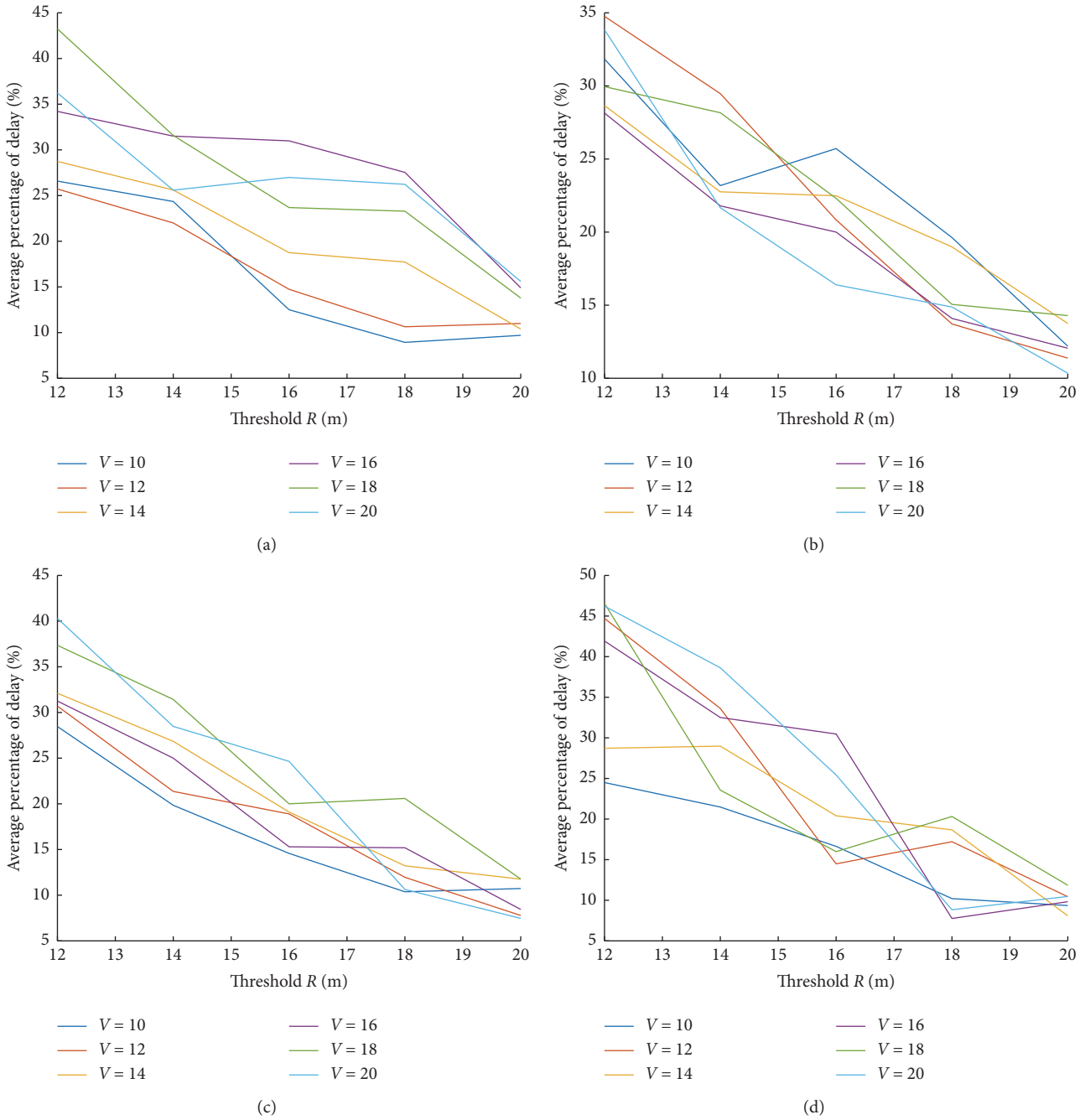

Figure 9: Continued.

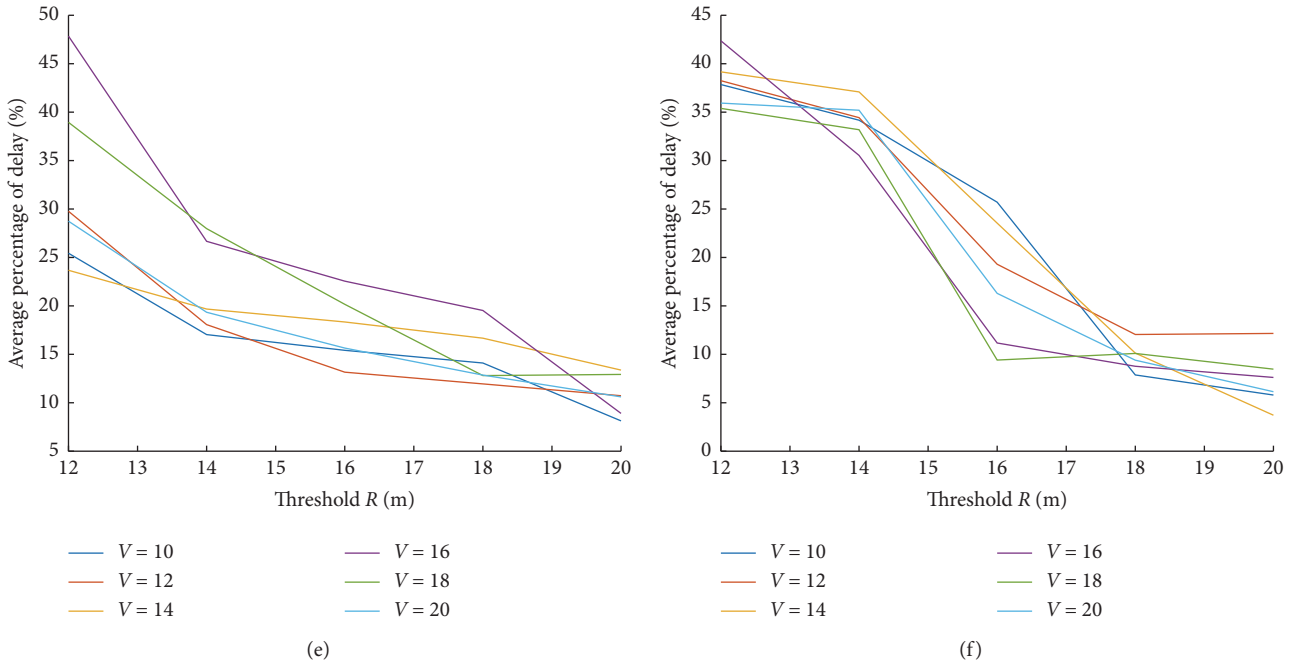

Figure 9: Average delay increment comparison for multi-UAV clusters of different sizes at a speed from 10 to 20 m/s and with R from 12 to 20 m. (a) Result for 5-UAV clusters. (b) Result for 6-UAV clusters. (c) Result for 7-UAV clusters. (d) Result for 8-UAV clusters. (e) Result for 9-UAV clusters. (f) Result for 10-UAV clusters.

Table 4: Average delay increment for 5-UAV clusters at a speed of 10–20 m/s and with R of 12–20 m.

Threshold R (m)	$V = 10$ m/s (%)	$V = 12$ m/s (%)	$V = 14$ m/s (%)	$V = 16$ m/s (%)	$V = 18$ m/s (%)	$V = 20$ m/s (%)
12	26.58	25.71	28.74	34.21	43.24	36.23
14	24.35	22.00	25.61	31.51	31.58	25.59
16	12.15	14.74	18.75	30.99	23.68	26.98
18	8.93	10.64	17.72	27.54	23.29	26.23
20	9.70	11.03	10.39	14.90	13.78	15.60

Table 5: Average delay increment for 6-UAV clusters at a speed of 10–20 m/s and with R of 12–20 m.

Threshold R (m)	$V = 10$ m/s (%)	$V = 12$ m/s (%)	$V = 14$ m/s (%)	$V = 16$ m/s (%)	$V = 18$ m/s (%)	$V = 20$ m/s (%)
12	31.84	34.76	28.65	28.14	29.95	33.85
14	23.18	29.47	22.75	21.79	28.17	21.67
16	25.71	20.83	22.49	20.01	22.31	16.39
18	19.63	13.71	18.99	14.09	15.05	14.88
20	12.20	11.38	13.75	12.06	14.29	10.34

Table 6: Average delay increment for 7-UAV clusters at a speed of 10–20 m/s and with R of 12–20 m.

Threshold R (m)	$V = 10$ m/s (%)	$V = 12$ m/s (%)	$V = 14$ m/s (%)	$V = 16$ m/s (%)	$V = 18$ m/s (%)	$V = 20$ m/s (%)
12	28.46	30.70	32.11	31.25	37.35	40.30
14	19.84	21.36	26.84	25.00	31.43	28.48
16	14.57	18.90	19.10	15.29	20.00	24.65
18	10.37	11.96	13.22	15.19	20.59	10.63
20	10.73	7.78	11.75	8.44	11.76	7.46

Table 7: Average delay increment for 8-UAV clusters at a speed of 10–20 m/s and with R of 12–20 m.

Threshold R (m)	$V = 10$ m/s (%)	$V = 12$ m/s (%)	$V = 14$ m/s (%)	$V = 16$ m/s (%)	$V = 18$ m/s (%)	$V = 20$ m/s (%)
12	24.50	44.71	28.72	41.93	46.56	46.22
14	21.48	33.62	28.98	32.51	23.56	38.63
16	16.64	14.48	20.41	30.47	15.99	25.43
18	10.20	17.21	18.67	7.76	20.32	8.83
20	9.35	10.44	8.09	9.82	11.84	10.47

Table 8: Average delay increment for 9-UAV clusters at a speed of 10–20 m/s and with R of 12–20 m.

Threshold R (m)	$V = 10$ m/s (%)	$V = 12$ m/s (%)	$V = 14$ m/s (%)	$V = 16$ m/s (%)	$V = 18$ m/s (%)	$V = 20$ m/s (%)
12	25.44	29.77	23.68	47.84	38.94	28.74
14	17.04	18.07	19.67	26.66	27.97	19.34
16	15.41	13.16	18.34	22.55	20.16	15.64
18	14.10	11.95	16.67	19.52	12.80	12.85
20	8.13	10.73	13.37	8.90	12.92	10.60

Table 9: Average delay increment for 10-UAV clusters at a speed of 10–20 m/s and with R of 12–20 m.

Threshold R (m)	$V = 10$ m/s (%)	$V = 12$ m/s (%)	$V = 14$ m/s (%)	$V = 16$ m/s (%)	$V = 18$ m/s (%)	$V = 20$ m/s (%)
12	37.84	38.24	39.15	42.36	35.38	35.93
14	34.16	34.43	37.08	30.53	33.18	35.19
16	25.70	19.29	23.54	11.17	9.40	16.29
18	7.87	12.04	10.12	8.76	10.09	9.39
20	5.79	12.15	3.71	7.61	8.46	6.14

Table 10: Comparison of different attack methods.

Method		Target	Attack effect
Physically	Son et al. [27]	Gyroscopic sensor	Crash
	Choi et al. [28]	GPS sensor	Path deviation
	Trippel et al. [29]	Accelerometers	Unstable flight
	Davidson et al. [20]	Optical flow sensor	Position error
	Tippenhauer et al. [19]	GPS sensor	Position error
Through malware	Dash et al. [11]	Software stack	Unstable flight
	Mazloom et al. [10]	Software stack	Unstable flight
Wirelessly	Highnam et al. [30]	Wireless channel	Disrupted communications
	Ghanavati et al. [31]	PDE algorithm	Time delay
	Our method	Flocking algorithm	Time delay

flight, which is still unacceptable in emerging tasks of monitoring, search, and rescue.

7.2. Autonomous UAV Cluster and Security. Privacy leak and collision are two common security issues for the UAV cluster. In the works [32–35], researchers studied privacy issues in UAV clusters, such as privacy refers to preventing the inference of the leader's identity in leader-follower structure swarms. Our work belongs to the latter security issue of flocking-based cluster and collision. Reynolds proposed the Boids model in 1986, which is the earliest flocking model [1]. Zaera et al. intended to develop neural network-based controllers for schooling behavior in three dimensions, using realistic Newtonian kinematics, such as inertia and drag [36]. Vicsek et al. proposed a particle swarm model [37], in which each particle moves at the same unit speed, and the direction is the average of the direction of its neighbor particles. Although this model only achieves the overall direction consistency of the particle swarm and ignores the collision avoidance of each particle, it still makes an important contribution to the modeling of swarm agents. Sharma and Ghose extended the Boids model and proposed a swarm intelligence algorithm to avoid cluster collisions [4].

One of the recent applications of the self-organized swarm intelligence algorithm is collective UAVs [38], where decentralized control algorithms for groups of autonomous

UAVs can be developed on the basis of interactions as a prerequisite for safe operation. In comparison, our attack target is based on the 5-policy flocking algorithm, which has more widespread applications.

The largest UAV cluster so far was developed by Ehang with more than 1000 UAVs. However, these UAVs were individually programmed for predefined trajectories or were centrally controlled and did not satisfy the autonomy with swarm intelligence [39]. The US military had an experiment with fixed-wing drone swarms called Perdix [40, 41]. Unfortunately, there is no public information about its control mechanisms, communication schemes, or possible collision avoidance behaviors to reliably evaluate. In comparison, we target a lab-level UAV cluster with 10 UAVs.

A previous related work is the intrusion detection-based multi-UAV mission execution [42]. In their method, a subflight area is demarcated by the coordinates of the waypoints in the assigned tasks of the UAV. According to the UAV's GPS coordinates, if the current UAV exceeds this area, it is considered suspicious and will cut off the connection with other UAVs, and the others reconnect. In comparison, our method focuses on flocking-based UAV collaboration, and we do not perform GPS spoofing but arrival status spoofing, which is a special parameter in the swarm intelligence of flocking.

8. Conclusions

In this work, we perform the first security analysis of the flocking algorithm that is most widely used in UAV clusters. Targeting a highly realistic threat model in AODV link authentication through rushing attack-based data spoofing, we perform vulnerability analysis and find that the current flocking algorithm design is highly vulnerable to data spoofing attacks. The evaluation results in the simulation environment validate the effectiveness of the attack and show that the attack can even cause nearly 50% arrival delay. Defense directions are then discussed leveraging the insights.

This work serves as a first step to understand the new security problems and challenges in the flocking, a main kind of swarm intelligence algorithm of UAVs. It is expected to inspire a series of follow-up studies, including but not limited to (1) more extensive evaluation with UAV clusters with different formation structures, (2) more extensive analysis considering other swarm intelligence algorithms, such as the one imitating bees or ants, and (3) more concrete defense approach and evaluation.

Data Availability

All data generated or analyzed during this study are owned by all the authors and will be used for further research. The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (61972025, 61802389, 61672092, U1811264, and 61966009), the Fundamental Research Funds for the Central Universities of China (2018JBZ103 and 2019RC008), Science and Technology on Information Assurance Laboratory (614200103011711), and Guangxi Key Laboratory of Trusted Software (KX201902).

Supplementary Materials

We provide a video file to show a simulated attack in MATLAB. In this attack scenario, there is a cluster of 8 UAVs with an applied flocking algorithm, keeping a formation from the left source to the right destination. A data spoofing through masquerading as the first-arrival UAV is performed at a location of 20-meter distance away from the destination, and then a heavy delay occurred among the following UAVs. Through the video supplementary material, we reveal the whole flying and attacking process. (*Supplementary Materials*)

References

[1] C. W. Reynolds, "Flocks, herds and schools: a distributed behavioral model," in *Proceedings of the 14th Annual Conference on Computer Graphics and Interactive Techniques*, pp. 25–34, Anaheim, CA, USA, August 1987.

[2] S.-J. Chung, A. A. Paranjape, P. Dames, S. Shen, and V. Kumar, "A survey on aerial swarm robotics," *IEEE Transactions on Robotics*, vol. 34, no. 4, pp. 837–855, 2018.

[3] D. Zhou, Z. Wang, and M. Schwager, "Agile coordination and assistive collision avoidance for quadrotor swarms using virtual structures," *IEEE Transactions on Robotics*, vol. 34, no. 4, pp. 916–923, 2018.

[4] R. K. Sharma and D. Ghose, "Collision avoidance between UAV clusters using swarm intelligence techniques," *International Journal of Systems Science*, vol. 40, no. 5, pp. 521–538, 2009.

[5] M. M. Zanjireh and H. Larijani, "A survey on centralised and distributed clustering routing algorithms for WSNs," in *Proceedings of the 81st IEEE Vehicular Technology Conference (VTC Spring)*, pp. 1–6, Glasgow, UK, May 2015.

[6] A. Bhattacharyya, A. Banerjee, D. Bose et al., *Different Types of Attacks in Mobile ADHOC Network: Prevention and Mitigation Techniques*, Department of Computer Science & Engineering, Institute of Engineering & Management, Saltlake, UT, USA, 2011.

[7] Y. C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," in *Proceedings of the 2nd ACM Workshop on Wireless Security*, pp. 30–40, San Diego CA USA, September 2003.

[8] K. Koscher, A. Czeskis, F. Roesner et al., "Experimental security analysis of a modern automobile," in *Proceedings of the 2010 IEEE Symposium on Security and Privacy*, pp. 447–462, IEEE, Oakland, CA, USA, May 2010.

[9] S. Checkoway, D. McCoy, B. Kantor et al., "Comprehensive experimental analyses of automotive attack surfaces," *USENIX Security Symposium*, vol. 4, pp. 447–462, 2011.

[10] S. Mazloom, M. Rezaeirad, A. Hunter et al., "A security analysis of an in-vehicle infotainment and app platform," in

Proceedings of the 10th USENIX Conference on Offensive Technologies, pp. 232–243, Austin, TX, USA, August 2016.

[11] P. Dash, M. Karimibiuki, and K. Pattabiraman, "Out of control: stealthy attacks against robotic vehicles protected by control-based techniques," in *Proceedings of the 35th Annual Computer Security Applications Conference*, pp. 660–672, San Juan, PR, USA, December 2019.

[12] H. Hildenbrandt, C. Carere, and C. K. Hemelrijk, "Self-organized aerial displays of thousands of starlings: a model," *Behavioral Ecology*, vol. 21, no. 6, pp. 1349–1359, 2010.

[13] D. Morgan, G. P. Subramanian, S.-J. Chung, and F. Y. Hadaegh, "Swarm assignment and trajectory optimization using variable-swarm, distributed auction assignment and sequential convex programming," *The International Journal of Robotics Research*, vol. 35, no. 10, pp. 1261–1285, 2016.

[14] 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.

[15] Y. Kantaros and M. M. Zavlanos, "Global planning for multi-robot communication networks in complex environments," *IEEE Transactions on Robotics*, vol. 32, no. 5, pp. 1045–1061, 2016.

[16] F. Van Breugel, K. Morgansen, and M. H. Dickinson, "Monocular distance estimation from optic flow during active landing maneuvers," *Bioinspiration & Biomimetics*, vol. 9, no. 2, Article ID 025002, 2014.

[17] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," *IEEE Communications Magazine*, vol. 40, no. 10, pp. 70–75, 2002.

[18] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki et al., "Assessing the spoofing threat: development of a portable GPS civilian spoofer," in *Proceedings of the Institute of Navigation GNSS*, pp. 1198–1209, Savannah, GA, USA, September 2008.

[19] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen et al., "On the requirements for successful GPS spoofing attacks," in *Proceedings of the 18th ACM Conference on Computer and Communications Security*, pp. 75–86, Chicago, IL, USA, October 2011.

[20] D. Davidson, H. Wu, R. Jellinek et al., "Controlling UAVs with sensor input spoofing attacks," in *Proceedings of the 10th USENIX Conference on Offensive Technologies*, pp. 221–231, Austin, TX, USA, August 2016.

[21] S. McLaughlin and S. Zonouz, "Controller-aware false data injection against programmable logic controllers," in *Proceedings of the 2014 IEEE international Conference on smart Grid communications (SmartGridComm)*, pp. 848–853, IEEE, Venice, Italy, November 2014.

[22] J. S. Warner and R. G. Johnston, "A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing," *Journal of Security Administration*, vol. 25, no. 2, pp. 19–27, 2002.

[23] W. Niu, J. Lei, E. Tong et al., "Context-aware service ranking in wireless sensor networks," *Journal of Network and Systems Management*, vol. 22, no. 1, pp. 50–74, 2014.

[24] W. Li, G. Li, Z. Zhao, H. Tang, and Z. Shi, "Multi-granularity context model for dynamic Web service composition," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 312–326, 2011.

[25] W. Niu, G. Li, H. Tang, X. Zhou, and Z. Shi, "CARSA: a context-aware reasoning-based service agent model for AI planning of web service composition," *Journal of Network and Computer Applications*, vol. 34, no. 5, pp. 1757–1770, 2011.

[26] E. Tong, W. Niu, G. Li et al., "Bloom filter-based workflow management to enable QoS guarantee in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 39, pp. 38–51, 2014.

[27] Y. Son, H. Shin, D. Kim et al., "Rocking drones with intentional sound noise on gyroscopic sensors," in *Proceedings of the 24th {USENIX} Security Symposium ({USENIX} Security 15)*, pp. 881–896, Washington, DC, USA, August 2015.

[28] H. Choi, W. C. Lee, Y. Aafer et al., "Detecting attacks against robotic vehicles: a control invariant approach," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 801–816, Toronto, Canada, October 2018.

[29] T. Trippel, O. Weisse, W. Xu et al., "WALNUT: waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks," in *Proceedings of the 2017 IEEE European symposium on security and privacy (EuroS&P)*, pp. 3–18, IEEE, Paris, France, April 2017.

[30] K. Highnam, K. Angstadt, K. Leach et al., "An uncrewed aerial vehicle attack scenario and trustworthy repair architecture," in *Proceedings of the 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W)*, pp. 222–225, IEEE, Toulouse, France, June 2016.

[31] M. Ghanavati, A. Chakravarthy, and P. Menon, "PDE-based analysis of cyber-attacks in vehicle swarms," in *Proceedings of the 2018 IEEE Conference on Decision and Control (CDC)*, pp. 1329–1334, IEEE, Miami Beach, FL, USA, December 2018.

[32] H. Zheng, J. Panerati, G. Beltrame, and A. Prorok, "An adversarial approach to private flocking in mobile robot teams," *IEEE Robotics and Automation Letters*, vol. 5, no. 2, pp. 1009–1016, 2020.

[33] A. Prorok and V. Kumar, "Privacy-preserving vehicle assignment for mobility-on-demand systems," in *Proceedings of the 2017 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pp. 1869–1876, Vancouver, Canada, September 2017.

[34] L. Li, A. Bayuelo, L. Bobadilla, T. Alam, and D. A. Shell, "Coordinated multi-robot planning while preserving individual privacy," in *Proceedings of the IEEE International Conference on Robotics and Automation*, pp. 2188–2194, Montreal, Canada, May, 2019.

[35] Y. Zhang and D. A. Shell, "Complete characterization of a class of privacy-preserving tracking problems," *The International Journal of Robotics Research*, vol. 38, no. 2-3, pp. 299–315, 2019.

[36] N. Zaera, D. Cliff, and J. Bruten, "(Not) Evolving collective behaviours in synthetic fish," in *Proceedings of the International Conference on the Simulation of Adaptive Behavior*, pp. 635–642, MIT Press, Cambridge, MA, USA, August 1996.

[37] T. Vicsek, A. Czirók, E. Ben-Jacob, I. Cohen, and O. Shochet, "Novel type of phase transition in a system of self-driven particles," *Physical Review Letters*, vol. 75, no. 6, pp. 1226–1229, 1995.

[38] M. Cohen, E. Ferrante, M. Birattari, and M. Dorigo, "Swarm robotics: a review from the swarm engineering perspective," *Swarm Intelligence*, vol. 7, no. 1, pp. 1–41, 2013.

[39] F. Y. Hadaegh, S. J. Chung, and H. M. Manohara, "On development of 100-gram-class spacecraft for swarm applications," *IEEE Systems Journal*, vol. 10, no. 2, pp. 673–684, 2014.

[40] G. Vásárhelyi, C. Virágh, G. Somorjai et al., "Optimized flocking of autonomous drones in confined environments," *Science Robotics*, vol. 3, pp. 1–13, 2018.

[41] R. Mitchell and I. R. Chen, "Specification based intrusion detection for unmanned aircraft systems," in *Proceedings of the First ACM MobiHoc Workshop on Airborne Networks and Communications*, pp. 31–36, Hilton Head, SC, USA, June 2012.

[42] Z. Fu, Y. Mao, D. He, J. Yu, and G. Xie, "Secure multi-UAV collaborative task allocation," *IEEE Access*, vol. 7, pp. 35579–35587, 2019.