IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 27, 2020, accepted April 22, 2020, date of publication April 29, 2020, date of current version May 14, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2991211

A Complex Networks Approach for Reliability Evaluation of Swarm Systems Under Malicious Attacks

KANGKAI LIU[1], JILONG ZHONG[2], GUANGHAN BAI[3], AND YI YANG[1]

[1]School of Reliability and Systems Engineering, Beihang University, Beijing 100191, China
[2]National Institute of Defense Technology Innovation, PLA Academy of Military Science, Beijing 100091, China
[3]Laboratory of Science and Technology on Integrated Logistics Support, College of Intelligence Science and Technology, National University of Defense Technology, Changsha 410073, China

Corresponding authors: Yi Yang (yang_cissy@163.com) and Jilong Zhong (z_jilong@sina.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61871013, Grant 61573041, and Grant 71701207, and in part by the Science and Technology on Reliability and Environmental Engineering Laboratory.

ABSTRACT The reliability of swarm systems needs to be investigated because of their self-adaption and self-organized features. Previous studies mainly focused on the reliability of a single agent, whereas for swarm systems, the ability to maintain their overall connection and function under adverse conditions is more important. It remains challenging on how to evaluate the reliability of swarm systems at the system level. In this paper, we present a reliability evaluation method for swarm systems by characterizing the behavior of the whole system using the method of temporal network analysis. A novel comprehensive reliability metric, i.e. cooperation reliability (CR), is proposed, considering both system integrity and motion consensus. Meanwhile, by identifying critical individuals in swarm systems, we design different malicious attack strategies. It is found that the malicious attacks perform much more harmfully to the reliability of swarm systems than noise and random attack. Moreover, we find that the reliability of a swarm system is sensitive to the swarm density in our framework due to the dynamical interaction of the system. Our findings may shed light on understanding the complicated behaviors of swarm systems under attack and designing a more robust swarm system.

INDEX TERMS Complex networks, malicious attacks, reliability, swarm system.

I. INTRODUCTION

Applications of swarm systems are emerging in various fields, showing clearly the importance of swarm systems. For instance, several UAV swarms, such as Gremlins, Coyote drones, and Perdix, are designed for military tasks like distributed reconnaissance, cooperative attack, and saturation attack; In the civilian field, swarm systems are being applied to distributed sensing, emergency rescue etc. These engineering applications take advantage of the superiority of swarm systems in information sharing, collaboration, and robustness, and require the swarm systems to be reliable. Beginning with the observation of behaviors of biological flocks, researchers have been studying swarm systems for decades. Researchers studied the swarm systems in nature [1]–[10] thoroughly and designed a number of artificial swarm systems [11]–[15] to achieve robustness, flexibility, scalability, and more importantly, superior capabilities of the whole system compared with single agents [13], [14]. However, under perturbations like noise or malicious attacks, swarm systems may become unstable and even collapse. Thus, the consensus of the system is difficult to maintain [16]–[21], creating security challenges [22], [23] and reliability concerns [24], [25].

Initially, researchers mainly focused on reliability of a single agent. Winfield *et al.* [24] proposed three different tentative approaches [25] to evaluate the reliability of a robot swarm. These approaches tried to evaluate the reliability of swarm system by the function of reliabilities of all the agents in the system, but ignored the system's self-adaption and self-organized features, since they were developed on an arbitrary assumption, that the whole system breaks down only if all of its individuals break down. Due to the dynamical change of system topology, usually the reliability function between

The associate editor coordinating the review of this manuscript and approving it for publication was Cristian Zambelli.

the swarm system and the single agent is absolutely different, especially under attack situation. The above problems constitute a major challenge as how to evaluate the overall reliability of swarm systems at the system level.

To study the topology and system-level ability of swarm systems, researchers employed complex network theory. They regard a swarm system as a network composed by the individuals (nodes) and the interactions among them (links), and analyze the network by statistical mechanics, graph theory, control theory etc. Using this methodology, Komareji and Bouffanais [18] found that the networks of their swarm model based on the k-nearest neighbor rules exhibit small-world effect and possess Poissonian-like indegree distribution, differing from the power law characteristic of scale-free networks. Moreover, researchers of swarm systems have gained extraordinary results in consensus problem [17], [26], information flow [26], [27], controllability [18], and resilience [18]–[21], [28]. In this paper, we expect that network-based methodology can help us to grasp the big picture of the whole system and develop a overall reliability evaluation approach for swarm systems.

The vulnerability of swarm systems is another compelling problem to study due to the network feature of swarm systems. Albert *et al.* [29] found that attacking highly connected nodes in a scale-free network can cause more significant damage to the topology than attacking those less connected ones, which revealed the attack vulnerability of scale-free networks. Jianwei Wang *et al.* proposed a cascading model to explain the attack vulnerability of scale-free networks [30]. Propagation of cascading failures [31], [32] and restoration from cascading failure [33]–[36] has been studied. After [29], a series of studies about attack tolerance or vulnerability of static networks [37]–[41] and temporal networks [42]–[47] emerged. Metrics like degree, closeness, betweenness etc. has been practiced to identify the significance of nodes [48], [49]. Nevertheless, faced with malicious attacks, whether the temporal network of a swarm system exhibits vulnerability just like scale-free networks do is uncertain.

In this paper, we model swarm systems based on the Vicsek model [16], where the function of the particles is ordered motion. We construct temporal networks for our swarm systems and define the system-level reliability of a swarm system as the ability to maintain swarm behavior, i.e. cooperation reliability (CR), which is a combination of system integrity and motion consensus. This is realistic for real situation. For example, UAV swarm with reconnaissance mission needs to transfer and exchange information with each other based on clusters in the system, where connection guarantees the interaction ability. Swarm also needs motion consensus in a self-adaptive formation flight for the ease of system control. To measure the cooperation reliability, the swarm all-terminal reliability (SATR) is defined to evaluate the integrity of the system and the consensus metric is introduced to evaluate the motion consensus of all the individuals. Moreover, using identification methods of vital nodes in complex networks, we design three attack strategies, including random attack and two malicious attack strategies, and study their influences on the reliability of our swarm systems. Specifically, we do not consider the reliability of individual particles, i.e. we assume that every single particle's reliability equals to 1. In all, our main contributions can be summarized as:

- A novel reliability metric is proposed, combining system integrity and motion consensus.
- We analyze the temporal networks of swarm systems based on percolation theory, considering the self-adaption and self-organized features of the network.
- We also study and compare the reliabilities and behaviors of swarm systems under different attack strategies.

The rest paper is organized as follows. We introduce the models in section II, including Vicsek model and temporal networks. Reliability metrics are proposed in section III and attack strategies are designed in section IV. We present and discuss our results in section V. Finally, we summarize this paper in section VI.

II. MODELS

A. VICSEK MODEL [16]

In this section, we describe some basic principles of the Vicsek model briefly and explain how we employ this model in this paper.

The Vicsek model consists of a square plane with periodic boundary conditions and N self-driven particles. These particles move continuously in the plane and their positions and directions of motion are updated at each time step. A particle's motion direction is calculated by averaging the directions of all the neighbors and then adding an external noise.

At a certain time step t, the neighbors of a particle i are all the nearby particles that are within a distance of r, represented by a set of particles $P_i(t)$,

$$P_i(t) = \left\{ j | d_{ij}(t) < r \right\}, \tag{1}$$

where d_{ij} denotes the distance from particle i to particle j. Parameter r can be considered as the maximum communication range among particles.

The direction of particle i is updated by the expression

$$\theta_i(t+1) = \langle \theta(t) \rangle_r + \Delta\theta_1, \quad \Delta\theta_1 \in [-\eta/2, \eta/2], \tag{2}$$

where $\theta_i(t+1)$ is the direction of particle i at step $t+1$, and $\Delta\theta_1$, denoting noise, is randomly chosen from the interval $[-\eta/2, \eta/2]$. In (2), $\langle \theta(t) \rangle_r$ represents the average of directions of all the neighbors of the given particle. If $\theta_j(t)$ represents the direction of particle j, then $\langle \theta(t) \rangle_r$ is subject to the expression

$$\begin{cases} \sin\langle \theta(t) \rangle_r = \frac{\sum_{j \in P_i(t)} \sin\theta_j(t)}{N_i(t)} \\ \cos\langle \theta(t) \rangle_r = \frac{\sum_{j \in P_i(t)} \cos\theta_j(t)}{N_i(t)} \end{cases}, \tag{3}$$

where $N_i(t)$ represents the number of the neighbors of particle i.

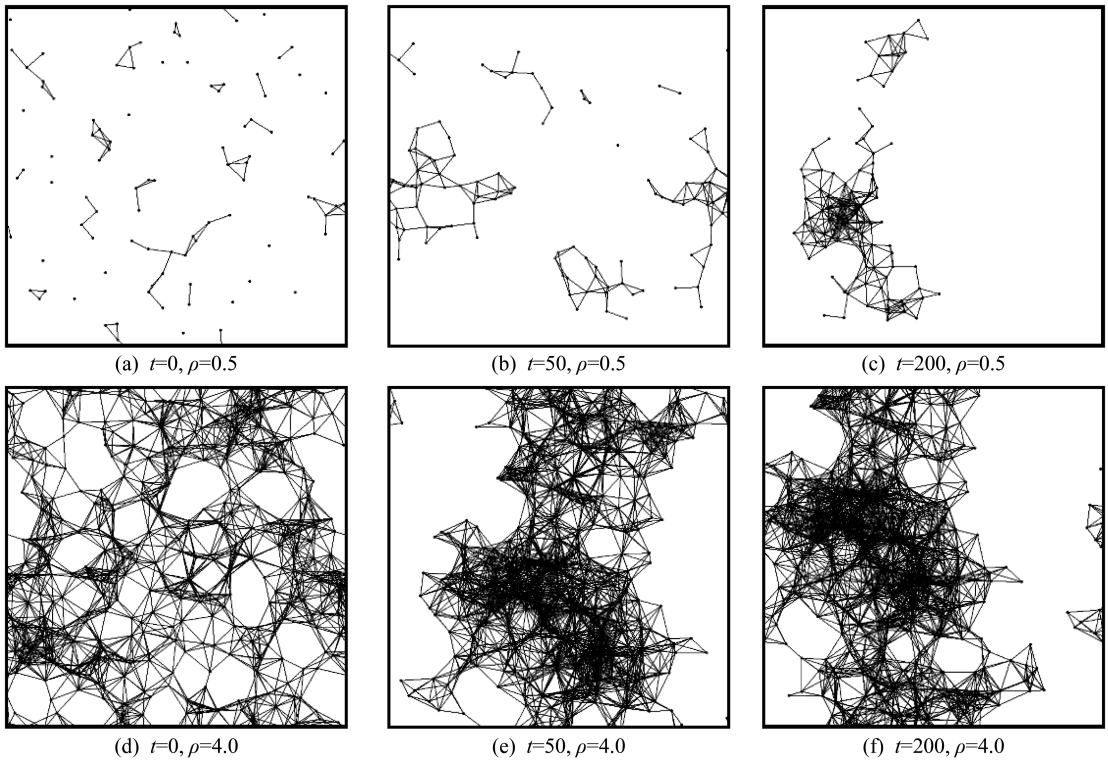


FIGURE 1. Evolving of swarm systems with different densities ρ. The networks of two swarm systems when time step [(a) and (d)] t=0, [(b) and (e)] t=50, and [(c) and (f)] t=200 in a simulation are shown. The other parameters used in these cases are: (a)-(c) the number of particles N=100 or (d)-(f) N=400, the length of the square cell is obtained by the expression $\rho=N/L^2$, the noise η=0, the speed v=0.03, and the communication range r=1.

Furthermore, $(x_i(t), y_i(t))$ represents the site of particle i, which is updated by the expression

$$\begin{cases} x_i(t+1)=x_i(t)+v\cos\theta_i(t+1) \\ y_i(t+1)=y_i(t)+v\sin\theta_i(t+1), \end{cases} \quad i=1,2\ldots,N, \qquad (4)$$

where v is the speed of all the particles.

B. TEMPORAL NETWORKS CONSTRUCTION

Represented by $G(t)=(V,E(t))$, the temporal network of a swarm system based on the Vicsek model is an unweighted and undirected graph at each time step. Node V_i in the networks represents particle i of the swarm system. $E(t)$ represents the interactions (links) among particles. A link fails when the distance between the two particles is larger than r. Here, the distance between particles means the Euclidean distance.

We show how the networks of swarm systems evolve in Fig. 1, with a case of low density and a case of high density. Initially, particles of the swarm system with low density are scattered in the field and the clusters are fragmented and dispersive (Fig. 1(a)). Gradually, those particles flock and construct large clusters as time passes (Fig. 1(b) and 1(c)). Whereas, in the other case, the swarm system's network maintains fully connected from the beginning to the end because of high swarm density.

III. RELIABILITY METRICS DEFINITION

The reliability of a system is the probability that it maintains its required function without failure under required work conditions for a given period of time [50]. For different swarm systems, their functions can be various: animal swarms need to migrate, hunt, or evade predators etc; artificial swarm systems can be employed to search and rescue victims, monitor or attack enemies etc. No matter what the specific function is, the swarm systems need to maintain swarm behavior. Here, we propose a method that describes the commonality of variant swarm systems. According to the definition of reliability referred in the beginning, we consider the swarm behavior as the required function of our swarm systems and the noise or malicious attacks as the potential required work conditions. The reliability of a swarm system is thus defined as the ability to maintain swarm behavior under required work conditions like noise or malicious attacks for a given period of time. Different from traditional reliability of electronic or mechanical systems, swarm reliability evaluation requires taking a full consideration on its highly dynamical, interdependent and resilient properties, revealing the profound relationship between swarm reliability and its properties. The failure of a single particle or a part of system may not collapse the system [18]. Therefore, swarm reliability evaluation needs to focus on the behavior of the whole system.

To measure the ability of a swarm system to maintain swarm behavior, we consider two aspects, system integrity and motion consensus. We believe that integrity and consensus are the two indispensable properties of swarm behavior. There are two reasons behind this thought. Firstly, the integrity (or wholeness) of a swarm system reflects the connection of its network, which is critical to the information sharing and the decision making. Secondly, the consensus ensures that the individuals in the swarm system act cooperatively. Our results reveal that under harsh conditions like strong noise or malicious attacks, neither of these two properties can guarantee the reliable operation of the system. In other words, in some cases, there exists gathered but disordered swarms or ordered but fragmented swarms. To evaluate the reliability of swarm systems, both integrity and consensus need to be considered.

Network methods are effective in studying the integrity of swarm systems. For instance, Komareji and Bouffanais [18] used the size of giant strongly connected component (GSCC) and the number of strongly connected components (SCC) as two integrity metrics to analyze the resilience of consensus in their model. We define swarm all-terminal reliability (SATR), which is inspired by the all-terminal reliability of networks, to evaluate the integrity of a swarm system in this paper. Compared with GSCC, the SATR describes the overall feature of the system rather than feature of the largest cluster. Given that every single particle's reliability equals to 1, we define SATR of swarm systems as follow.

Definition 1: Swarm All-terminal Reliability $SATR(t)$, the probability that each pair of particles are connected by at least one path. At time step t, if the swarm system is composed of N particles and $m(t)$ clusters, where each cluster contains $N_1, N_2, \ldots, N_{m(t)}$ particles respectively, the $SATR(t)$ of this swarm system is obtained from the expression

$$SATR(t) = \frac{\sum_{j=1}^{m(t)} \binom{N_j}{2}}{\binom{N}{2}}, \tag{5}$$

where $\binom{N_j}{2}$ is the 2-combination of cluster j and $\binom{N}{2}$ is the 2-combination of the whole system. Note that SATR is very different from the traditional ATR of a static network. Traditional ATR is probability of each pair of nodes being connected given the probability of failure for each link. However, SATR emphasizes the number of clusters in the system. Cluster size distribution is significant in percolation theory [51], [52], which captures the features of phase transition. Fewer clusters means a more integrated of the system and vice versa. The cluster statistics is widely used in traditional swarm system analyses [53]–[55]. SATR is the overall characterization of cluster statistics. When the system only has one cluster, i.e., $m(t) = 1$, $SATR(t)$ reaches its maximal value 1. When all particles disconnect from the system, i.e., $m(t) = N$, $SATR(t) = 0$. Thus, SATR is more suitable and objective to describe the swarm system. On the other hand, we use the order parameter that Vicsek *et al.* used in [16] as consensus metric to measure the motion consensus.

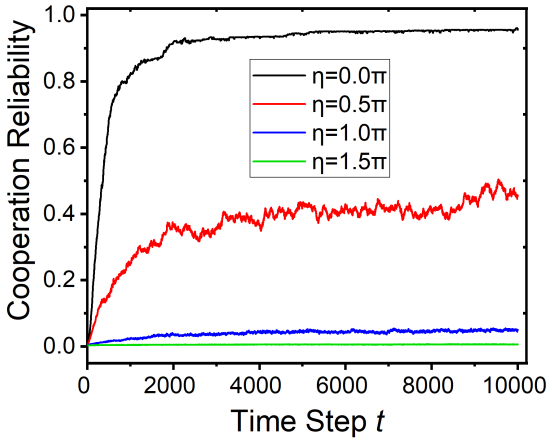


FIGURE 2. Cooperation reliability of swarm systems as the system evolving. Results of several levels of noise η are shown. The values of cooperation reliability are average over 100 realizations and in each realization the model runs for 10000 steps. The other parameters used in these cases are: the number of particles N=100, the length of the square cell L=14.1, the speed v=0.03, and the communication range r=1.

Definition 2: Consensus metric $V_a(t)$, the average velocity of the whole swarm system [16],

$$V_a(t) = \frac{1}{N}\left|\sum_{i=1}^{N} \vec{v_i}\right|, \tag{6}$$

where N is the number of particles in the system and $\vec{v_i}$ is the normalized velocity of particle i. $V_a(t)$ is approximately 0 when the directions of all the particles are totally unordered. When they move toward the same direction, $V_a(t) = 1$.

To evaluate the reliability of swarm systems comprehensively, we define the cooperation reliability (CR) as the reliability metric as follow.

Definition 3: Cooperation Reliability $CR(t)$, the ability of a swarm system to maintain swarm behavior at the time step t. We calculate $CR(t)$ by the expression

$$CR(t) = SATR(t) \times V_a(t). \tag{7}$$

Fig. 2 shows how the cooperation reliability converges as the system evolving. The stronger noise, the lower steady value of the cooperation reliability.

IV. ATTACK STRATEGIES

To simulate the potential external attacks on swarm systems, different attack strategies are considered. They are expected to destroy the swarm behavior of swarm systems as efficiently as possible. Let p denote the proportion of the attacked particles, then the number of the attacked particles is denoted by $N \times p$. The attacks on particles are adopted by disturbing their moving directions. The direction of an attacked particle, particle i, is updated by the expression

$$\tilde{\theta}_i\,(t+1) = \theta_i(t+1) + \Delta\theta_2, \qquad \Delta\theta_2 \in [-\pi, \pi], \tag{8}$$

where $\tilde{\theta}_i\,(t+1)$ denotes the direction under attack and $\theta_i(t+1)$ is the direction obtained from (2). Similar to angle $\Delta\theta_1$, $\Delta\theta_2$

is also a uniform distribution random number within the given interval and it denotes the external attack.

Then the location of the attacked particle i is updated by

$$\begin{cases} x_i(t+1) = x_i(t) + v\cos\tilde{\theta}_i\,(t+1) \\ y_i(t+1) = y_i(t) + v\sin\tilde{\theta}_i\,(t+1), \end{cases} \quad i = 1, 2 \ldots, N. \quad (9)$$

Notably, the noise and the attacks both influence the swarm behavior by disturbing the moving directions of particles, but the differences between them are remarkable. (i) Firstly, the noise is added on all the particles in the system, whereas the attacks only influence a part of particles. (ii) Secondly, usually the strength and effect of noise is relatively mild, whereas the attacks are much stronger. In our study, the attacks on a particle can be intuitively interpreted as 2π noise on this particle. No matter which attack strategy we employ, the way to update the directions of the attacked particles are the same, that is to update the directions according to (8). The difference lies in the selections of the attacked particles. Next, we will introduce three different attack strategies based on different methods of selection.

A. RANDOM ATTACK

In random attack (RA), the attacked particles are randomly chosen from all the particles, ignoring their positions or any other properties. This strategy is designed as a comparison of the malicious attacks presented subsequently. Moreover, the random attack can simulate the failures of individuals in the swarm system. In robot swarm systems, for example, failures of communication module or motion module can cause such errors of direction updating we designed by (8).

B. MALICIOUS ATTACKS

To break down the swarm systems efficiently, the malicious attacks target those vital particles, using vital nodes identification methods of complex networks. We rank all the particles decreasingly according to a certain temporal network property and then select the top $N \times p$ particles to attack. We define two specific malicious strategies using different temporal metrics as follow.

1) TEMPORAL DEGREE ATTACK

For a certain node V_i, its degree is the number of other nodes that directly connects to it [48]. Nodes connected to more nodes are more vital in some cases since they are able to affect more nodes. Since all the particles are moving, the degree of each particle is time-varying. Therefore, we define the temporal degree $D_i(t)$ as the degree of node V_i at a certain time step t. Under this strategy, the particles are ranked by their temporal degrees. We call this strategy degree attack (DA) for short in the rest of this paper.

2) TEMPORAL CLOSENESS CENTRALITY ATTACK

The closeness centrality of networks tries to identify the particles that are the closest to the information flow. The particles with higher closeness centralities are closer to the center of a network. Since the networks of swarm systems can be fragmented, we adopt the definition of closeness centrality in (10) [48], which is applicable to both fully connected networks and fragmented networks. For the node V_i of a network with N nodes, the closeness centrality is calculated by the expression

$$CC_i = \sum_{1 \le i < j \le N} \frac{1}{l_{ij}}, \quad (10)$$

where l_{ij} denotes the distance between V_i and V_j. Here, the distance represents the length of the shortest path between these two nodes. Particularly, if node V_i and node V_j are not connected, the distance between them equals to infinity. The temporal closeness centrality $CC_i(t)$ represents the closeness centrality of node V_i at a certain time step t. The strategy that attacks particles in terms of their closeness centralities is called closeness attack (CA) for short.

V. RESULTS AND DISCUSSION

We investigate the evolvement and reliability of swarm systems under various conditions. The results show how the noise and different attack strategies affect the integrity and the consensus of swarm systems. The average of the cooperation reliability, $\langle CR \rangle$, is obtained by

$$\langle CR \rangle = \langle SATR \rangle \times \langle V_a \rangle, \quad (11)$$

where $\langle SATR \rangle$ denotes the average of $SATR$ and $\langle V_a \rangle$ denotes the average of V_a over the 100 realizations.

A. NOISE EFFECT

The effects of noise on the motion consensus of swarm systems have been studied by Vicsek *et al.* [16] and Czirók and Vicsek [56]. Nevertheless, how noise influences the integrity of a swarm system is unclear. Komareji and Bouffanais [18] studied the evolvement of the size of GSCC and the number of SCC, yet they only presented the result of a fixed noise.

Fig. 3 shows the behaviors of particles under various noises. Firstly, from the perspective of single particles, the trajectories of particles under stronger noise are more winding. As a result, particles under stronger noise travel less distance by the same steps. Particularly, the particles under 2π rad noise (the highest noise) just linger in small regions around their original locations, because the noise is so strong. Secondly, from the perspective of the entire system, the swarm system under stronger noise is more fragmented, indicating lower $SATR$, and trajectories of all the particles are more disordered, namely lower V_a. Also, under stronger noise, the particles are more scattered (Fig. 3(a)-3(c)), resulting from the disturbance of the noise on the swarm behavior.

To investigate the effects of noise quantitatively, we calculate $SATR$, V_a, and CR of swarm systems with various densities under various levels of noise. We find that the stronger the noise, the lower $SATR$, V_a, and CR (Fig. 4). The reason is that under noise, the swarm systems are easier to break apart.

Moreover, Fig. 4 shows that under the same noise, the swarm systems with higher densities always exhibit

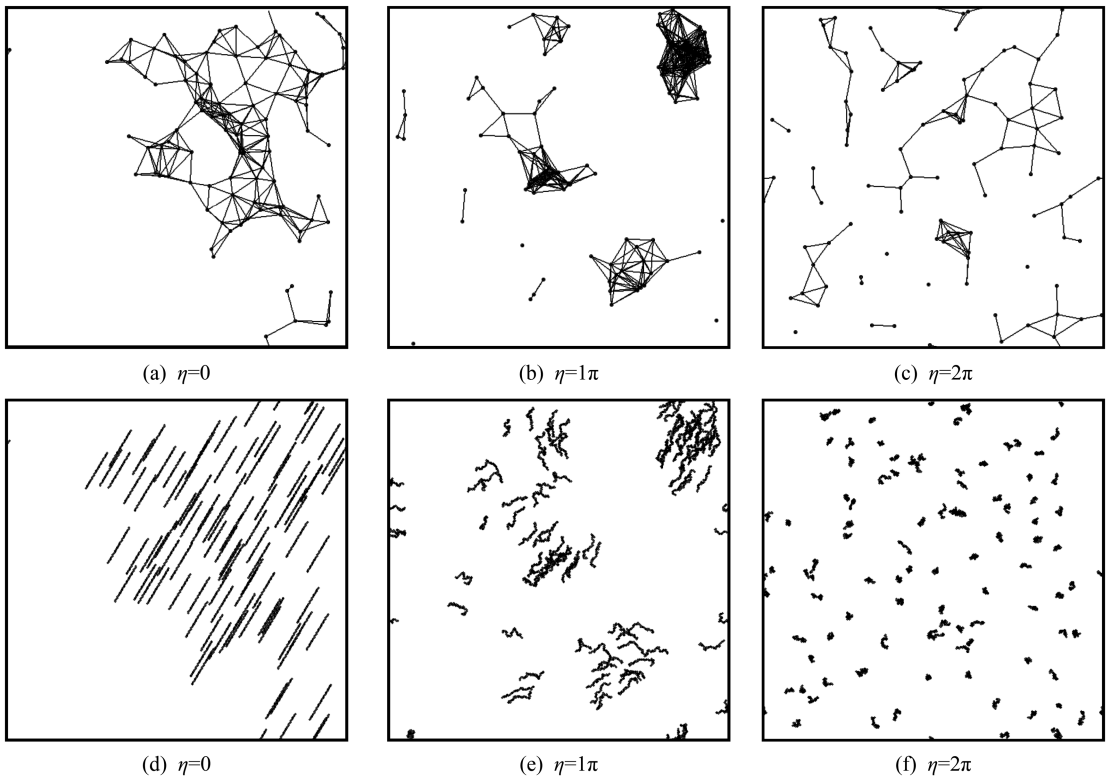


FIGURE 3. Effect of noise on swarm systems. (a)-(c) The networks of swarm systems under various noises η after simulation of 10000 steps and (d)-(f) their particles' trajectories of the last 40 steps are shown. The swarm in (a) and (d) is under the noise η=0; the swarm in (b) and (e) is under the noise η=1π; the swarm in (c) and (f) is under the noise η=2π. The other parameters used in these cases are: the number of particles N=100, the length of the square cell L=10, the speed v=0.03, and the communication range r=1.

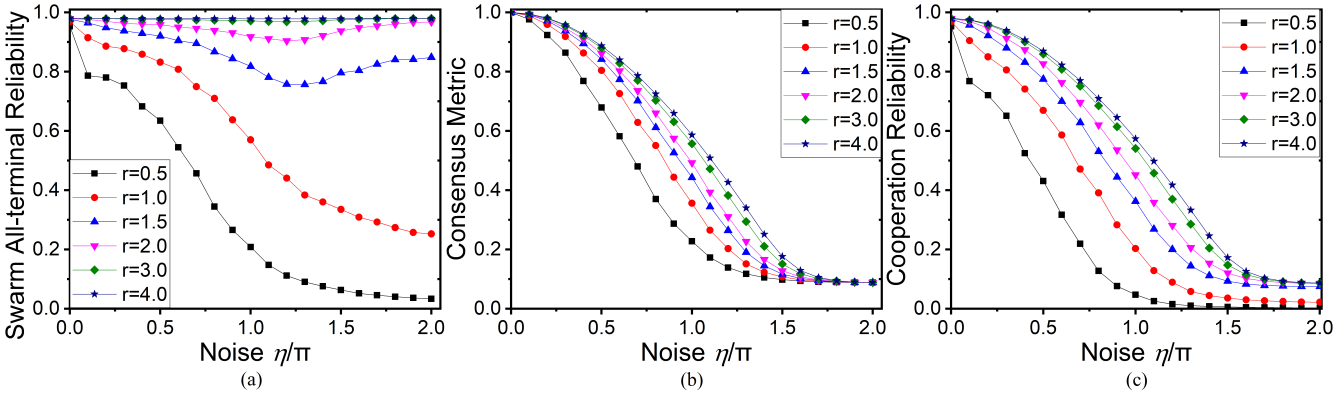


FIGURE 4. Effect of noise on the reliability of swarm systems. (a) Swarm all-terminal reliability, (b) consensus metric and (c) cooperation reliability of swarm systems with various density ρ are shown. The other parameters used in these cases are: the number of particles N=100, the density $\rho=N/L^2$, the speed v=0.03, and the communication range r=1.

higher *SATR*, V_a, and *CR*, which means the swarm systems with higher densities are more reliable. The fact is, when the density is higher, the particles are more likely to connect with each other. The density also influences *SATR*. When the density is high, *SATR* anti-intuitively increases as strong noise increases (Fig. 4(a)). (i) When the noise is weak, the system still maintains swarm behavior. With the strengthening of the noise, the networks are fragmented more severely, so *SATR* reduces. (ii) However, when the noise is strong enough, the swarm behavior vanishes and the particles are scattered. Given that the density is very high, the more scattered distribution of the particles makes it easier for the particles to connect with each other, so *SATR* anti-intuitively increases. Yet the particles do not achieve motion consensus in such case. More visually, the network of a high-density swarm system under strong noise is similar to the network in Fig. 1(d). This finding reveals the disadvantage of merely SATR in evaluating the reliability of swarm systems, that

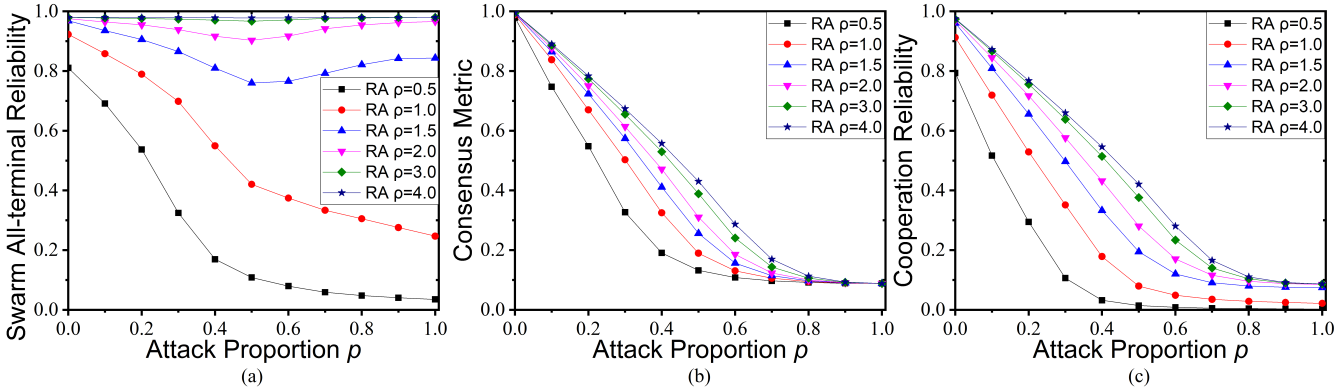


FIGURE 5. Effect of random attack (RA) on the reliability of swarm systems. (a) Swarm all-terminal reliability, (b) consensus metric and (c) cooperation reliability of swarm systems are shown. The other parameters used in these cases are: the number of particles N=100, the density ρ=N/L^2, the noise η=0.1π, the speed v=0.03, and the communication range r=1.

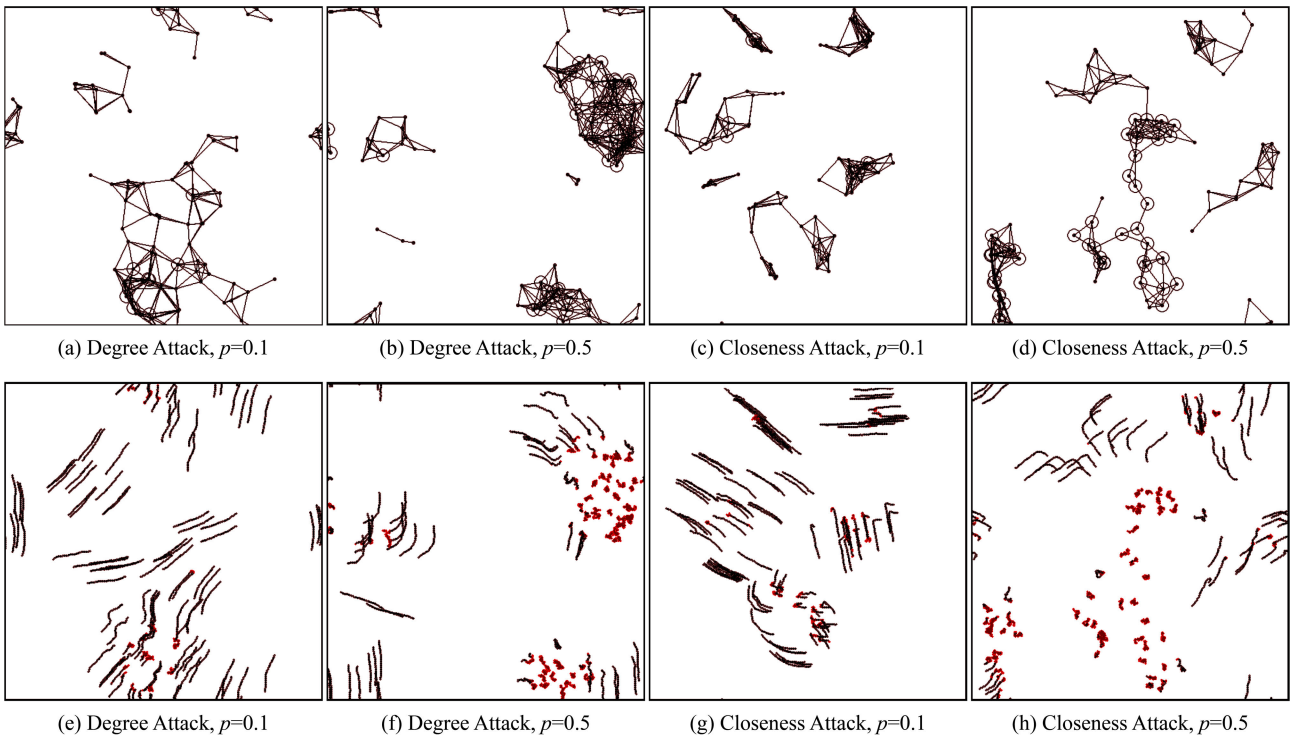


FIGURE 6. Effect of malicious attacks on swarm systems. (a)-(d) The networks of four swarm systems after 10000 steps of simulation and (e)-(h) their particles' trajectories of the last 40 steps are shown. The attacked particles are marked by circles. The swarm system in (a) and (e) is under degree attack (DA), with attack proportion p=0.1; the swarm system in (b) and (f) is under degree attack, with attack proportion p=0.5; the swarm system in (c) and (g) is under closeness attack (CA), with attack proportion p=0.1; the swarm system in (d) and (h) is under closeness attack, with attack proportion p=0.5. The other parameters used in these cases are: the number of particles N=100, the noise η=0.1π, the length of the square cell L=10, the speed v=0.03, and the communication range r=1.

it cannot tell whether the particles flock or just gather disorderly. Moreover, when the noise η increases from 0 to 0.1π, the consensus metric V_a just decays a little, whereas *SATR* declines much more significantly (Fig. 4(a) and 4(b)), which indicates that the consensus metric V_a is not enough to evaluate the reliability of swarm systems either.

B. EFFECTS OF ATTACK STRATEGIES

1) RANDOM ATTACK

The reliability of swarm systems under random attack with various failure proportion p and density ρ has been studied. Normally, *SATR* decreases as the failure proportion p grows (Fig. 5(a)). The consensus metric and the cooperation reliability monotonically decrease as p increases (Fig. 5(b) and 5(c)).

2) MALICIOUS ATTACKS

Malicious attacks are expected to break down the swarm systems efficiently. To investigate their impacts, we first observe the networks of the swarm systems under malicious attacks and the trajectories of the particles in Fig. 6.

It shows that the swarm systems under malicious attacks are more fragmented and the motions of their particles are

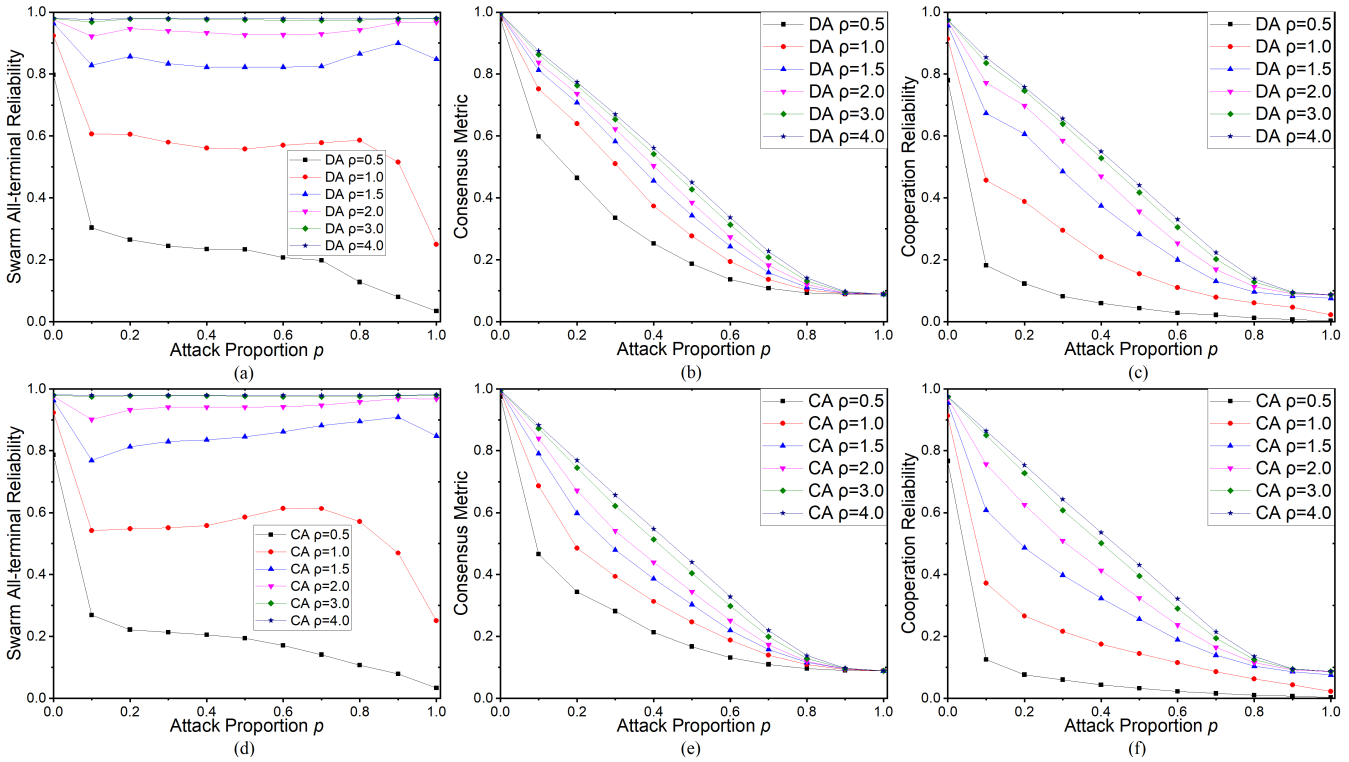


FIGURE 7. Effect of malicious attacks on the reliability of swarm systems. [(a) and (d)] Swarm all-terminal reliability, [(b) and (e)] consensus metric, and [(c) and (f)] cooperation reliability of swarm systems under degree attack (DA) or closeness attack (CA) are shown. The other parameters used in these cases are: the number of particles N=100, the density $\rho=N/L^2$, the noise $\eta=0.1\pi$, the speed v=0.03, and the communication range r=1.

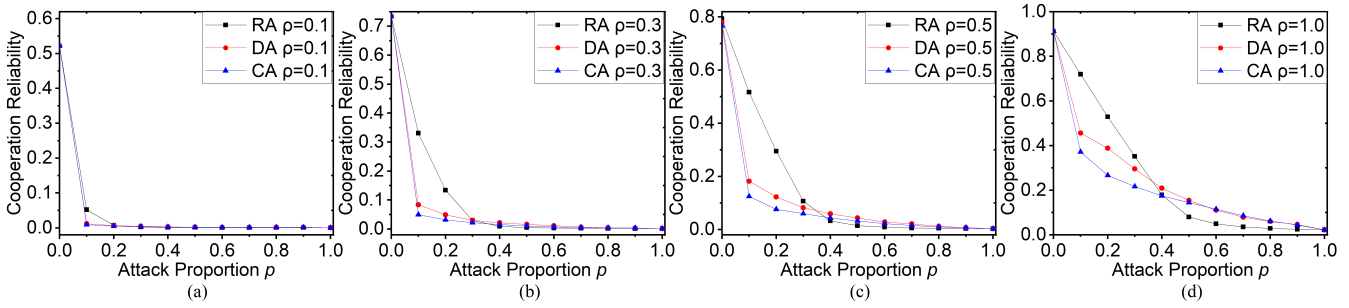


FIGURE 8. Comparison of effects of random attack (RA), degree attack (DA), and closeness attack (CA). Cooperation reliability of swarm systems with various densities ρ are shown. The densities of the swarm systems are equal to (a) 0.1, (b) 0.3, (c) 0.5, and (d) 1.0 respectively. The other parameters used in these cases are: the number of particles N=100, the density $\rho=N/L^2$, the noise $\eta=0.1\pi$, the speed v=0.03, and the communication range r=1.

more disordered, compared with the swarm systems only under noise in Fig. 3(a) and 3(d). However, we also notice that the attacked particles usually gather together without motion consensus, as shown in Fig. 6 by their trajectories. We call this phenomenon the disordered gathering of attacked particles.

As for reliability of swarm systems, Fig. 7 shows that *SATR*, V_a, and *CR* suffer serious damages under the malicious attacks, even when the attack proportion is small. Whereas, due to the disordered gathering of attacked particles, increasing the attack proportion cannot enlarge the much damage on *SATR*. It can even be counterproductive when the density is too high (Fig. 7(a)).

Furthermore, trends of these metrics with different densities exhibit subtle diversities. The *SATR*, V_a, and *CR* decrease more significantly in the swarm systems with lower densities, indicating that the swarm systems with lower densities are more vulnerable.

C. COMPARISON OF THREE ATTACK STRATEGIES

Fig. 8 presents the comparison of three attack strategies with various attack proportions. The *CR* of swarm systems under malicious attacks are lower than that under the random attack. This diversity shows that (1) the malicious attacks are more efficient to break down the swarm systems than random attack and (2) some particles are more critical to the whole

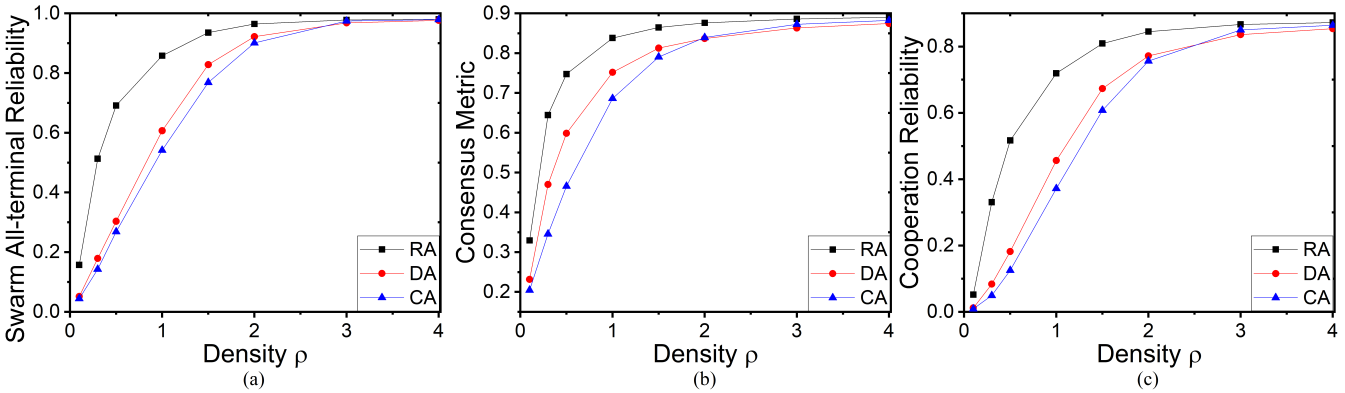


FIGURE 9. Comparison of effects of random attack (RA), degree attack (DA), and closeness attack (CA) with fixed attack proportion 0.1. (a) Swarm all-terminal reliability, (b) consensus metric and (c) cooperation reliability of swarm systems are shown. The densities ρ of the swarm systems are equal to 0.1, 0.3, 0.5, 1.0, 1.5, 2.0, 3.0, and 4.0 respectively. The other parameters used in these cases are: the attack proportion p=0.1, the number of particles N=100, the density $\rho=N/L^2$, the noise η=0.1π, the speed v=0.03, and the communication range r=1.

system than others, though there is no difference in their individual functions or performances. Moreover, between two malicious strategies, the closeness attack is more efficient than the degree attack, suggesting that the particles with high closeness centralities are more critical than the particles with high degrees. To compare the effects of these three attack strategies further, we investigate *SATR*, V_a, and *CR* with a fixed attack proportion $p = 0.1$, where we notice the highest difference among effects of these three attack strategies. Fig. 9 reveals that no matter for *SATR*, V_a, or *CR*, malicious attacks perform better attack effect than random attack. The particles with high degree or high closeness centrality are able to influence more particles. Thus, they are more important for the swarm systems to maintain swarm behavior. Meanwhile, within the framework of Vicsek model, the superiority of closeness attack over degree attack reveals that the importance of individuals is not only related to the number of neighbors (or degrees), but more importantly, the average distance to the other individuals, i.e. the location in the whole system.

VI. CONCLUSION

In this paper, we propose a novel reliability evaluation method for swarm systems by characterizing the system behavior, considering system integrity and motion consensus jointly. Compared with previous reliability metrics of swarm systems, the cooperation reliability emerges from the interaction among agents, reflecting the self-adaption and self-organized features of swarm behavior. This method is widely applicable for various swarm systems since it describes the commonality of different swarm systems. Moreover, to demonstrate this method, we study the reliability of swarm systems based on the Vicsek model under adverse work conditions including noise, random attack, and malicious attacks. The malicious attacks are designed by vital nodes identification in complex network. Simulation results show that the cooperation reliability comprehensively reflects the swarm system's ability to maintain its function under different work conditions. Also found is the vulnerability of swarm systems under malicious attacks, which indicates that misbehavior of different individuals influences behavior of the whole system differently, due to diverse locations in the system or connections to other individuals. This finding can be helpful for developing attack or protection strategies of swarm systems.

Yet, the malicious attack strategies designed in this paper have some shortcomings, since it is difficult for attackers to obtain the time-varying topology information of the swarm networks instantly. We will study the structural formation pattern of dynamic swarm networks in the future, try to uncover the relevance between failures and the structure of a dynamic swarm system in terms of topology changes and timing sequence, and further design a more robust swarm system.

REFERENCES

[1] C. W. Reynolds, "Flocks, herds and schools: A distributed behavioral model," *ACM SIGGRAPH Comput. Graph.*, vol. 21, no. 4, pp. 25–34, Aug. 1987.

[2] J. Toner and Y. Tu, "Flocks, herds, and schools: A quantitative theory of flocking," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 58, no. 4, pp. 4828–4858, Oct. 1998.

[3] D. Helbing, I. Farkas, and T. Vicsek, "Simulating dynamical features of escape panic," *Nature*, vol. 407, no. 6803, pp. 487–490, Sep. 2000.

[4] R. Olfati-Saber, "Flocking for multi-agent dynamic systems: Algorithms and theory," *IEEE Trans. Autom. Control*, vol. 51, no. 3, pp. 401–420, Mar. 2006.

[5] I. Giardina, "Collective behavior in animal groups: Theoretical models and empirical studies," *HFSP J.*, vol. 2, no. 4, pp. 205–219, Aug. 2008.

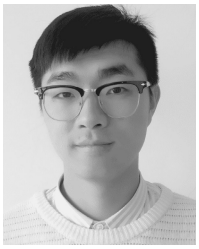
[6] M. Ballerini, N. Cabibbo, R. Candelier, A. Cavagna, E. Cisbani, I. Giardina, V. Lecomte, A. Orlandi, G. Parisi, A. Procaccini, M. Viale, and V. Zdravkovic, "Interaction ruling animal collective behavior depends on topological rather than metric distance: Evidence from a field study," *Proc. Nat. Acad. Sci. USA*, vol. 105, no. 4, pp. 1232–1237, Jan. 2008.

[7] M. Nagy, Z. Ákos, D. Biro, and T. Vicsek, "Hierarchical group dynamics in pigeon flocks," *Nature*, vol. 464, no. 7290, pp. 890–893, Apr. 2010.

[8] J. R. Usherwood, M. Stavrou, J. C. Lowe, K. Roskilly, and A. M. Wilson, "Flying in a flock comes at a cost in pigeons," *Nature*, vol. 474, no. 7352, pp. 494–497, Jun. 2011.

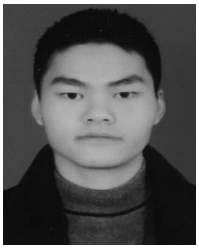
[9] S. Marras, S. S. Killen, J. Lindström, D. J. McKenzie, J. F. Steffensen, and P. Domenici, "Fish swimming in schools save energy regardless of their spatial position," *Behav. Ecology Sociobiol.*, vol. 69, no. 2, pp. 219–226, Feb. 2015.

[10] P. Corcoran and C. B. Jones, "Modelling topological features of swarm Behaviour in space and time with persistence landscapes," *IEEE Access*, vol. 5, pp. 18534–18544, 2017.
[11] H. Asama, *Distributed Autonomous Robotic Systems*. vol. 8. Berlin, Germany: Springer, 2009.
[12] A. L. Christensen, R. O'Grady, and M. Dorigo, "From fireflies to fault-tolerant swarms of robots," *IEEE Trans. Evol. Comput.*, vol. 13, no. 4, pp. 754–766, Aug. 2009.
[13] M. A. Joordens and M. Jamshidi, "Consensus control for a system of underwater swarm robots," *IEEE Syst. J.*, vol. 4, no. 1, pp. 65–73, Mar. 2010.
[14] L. Bayındır, "A review of swarm robotics tasks," *Neurocomputing*, vol. 172, pp. 292–321, Jan. 2016.
[15] G. Vásárhelyi, C. Virágh, G. Somorjai, T. Nepusz, A. E. Eiben, and T. Vicsek, "Optimized flocking of autonomous drones in confined environments," *Sci. Robot.*, vol. 3, no. 20, Jul. 2018, Art. no. eaat3536.
[16] T. Vicsek, A. Czirók, E. Ben-Jacob, I. Cohen, and O. Shochet, "Novel type of phase transition in a system of self-driven particles," *Phys. Rev. Lett.*, vol. 75, no. 6, pp. 1226–1229, Aug. 1995.
[17] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," *IEEE Trans. Autom. Control*, vol. 57, no. 1, pp. 90–104, Jan. 2012.
[18] M. Komareji and R. Bouffanais, "Resilience and controllability of dynamic collective behaviors," *PLoS ONE*, vol. 8, no. 12, 2013, Art. no. e82578.
[19] D. Han, Y. Mo, and L. Xie, "Towards a unified resilience analysis: State estimation against integrity attacks," in *Proc. 35th Chin. Control Conf. (CCC)*, Jul. 2016, pp. 7333–7340.
[20] G. Primiero, E. Tuci, J. Tagliabue, and E. Ferrante, "Swarm attack: A self-organized model to recover from malicious communication manipulation in a swarm of simple simulated agents," in *Swarm Intelligence* (Lecture Notes in Computer Science), vol. 1, M. Dorigo, M. Birattari, C. Blum, A. L. E. Christensen, A. Reina, and V. Trianni, Eds., Cham, Switzerland: Springer, 2018, pp. 213–224.
[21] I. Sargeant and A. Tomlinson, "Review of potential attacks on robotic swarms," in *Proc. SAI Intell. Syst. Conf.* in (Lecture Notes in Networks and Systems), vol. 2, Y. Bi, S. Kapoor, and R. Bhatia, Eds., Cham, Switzerland: Springer, 2018, pp. 628–646.
[22] M. Vahidalizadehdizaj, J. Jadav, and L. Tao, "Security challenges in swarm intelligence," in *Proc. 6th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2015, pp. 1–4.
[23] L. Petnga and H. Xu, "Security of unmanned aerial vehicles: Dynamic state estimation under cyber-physical attacks," in *Proc. Int. Conf. Unmanned Aircr. Syst. (ICUAS)*, Jun. 2016, pp. 811–819.
[24] A. F. T. Winfield, C. J. Harper, and J. Nembrini, "Towards dependable swarms and a new discipline of swarm engineering," in *Swarm Robotics* (Lecture Notes in Computer Science), D. Hutchison, Eds. Berlin, Germany: Springer, 2005, pp. 126–142.
[25] A. F. T. Winfield and J. Nembrini, "Safety in numbers: Fault-tolerance in robot swarms," *Int. J. Model., Identificat. Control*, vol. 1, no. 1, p. 30, 2006.
[26] R. Olfati-Saber, J. A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proc. IEEE*, vol. 95, no. 1, pp. 215–233, Jan. 2007.
[27] B. Blonder and A. Dornhaus, "Time-ordered networks reveal limitations to information flow in ant colonies," *PLoS ONE*, vol. 6, no. 5, 2011, Art. no. e20298.
[28] G. Bai, Y. Li, Y. Fang, Y.-A. Zhang, and J. Tao, "Network approach for resilience evaluation of a UAV swarm by considering communication limits," *Rel. Eng. Syst. Saf.*, vol. 193, Jan. 2020, Art. no. 106602.
[29] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, Jul. 2000.
[30] J. Wang, L. Rong, L. Zhang, and Z. Zhang, "Attack vulnerability of scale-free networks due to cascading failures," *Phys. A, Stat. Mech. Appl.*, vol. 387, no. 26, pp. 6671–6678, Nov. 2008.
[31] L. Daqing, J. Yinan, K. Rui, and S. Havlin, "Spatial correlation analysis of cascading failures: Congestions and blackouts," *Sci. Rep.*, vol. 4, no. 1, p. 5381, May 2015.
[32] J. Zhao, D. Li, H. Sanhedrai, R. Cohen, and S. Havlin, "Spatio-temporal propagation of cascading overload failures in spatially embedded networks," *Nature Commun.*, vol. 7, no. 1, Apr. 2016, Art. no. 010094.
[33] J. Wang, "Mitigation strategies on scale-free networks against cascading failures," *Phys. A, Stat. Mech. Appl.*, vol. 392, no. 9, pp. 2257–2264, May 2013.
[34] C. Liu, D. Li, E. Zio, and R. Kang, "A modeling framework for system restoration from cascading failures," *PLoS ONE*, vol. 9, no. 12, 2014, Art. no. e112363.
[35] C. Liu, D. Li, B. Fu, S. Yang, Y. Wang, and G. Lu, "Modeling of self-healing against cascading overload failures in complex networks," *EPL (Europhys. Lett.)*, vol. 107, no. 6, p. 68003, Sep. 2014.
[36] J. Zhong, F. Zhang, S. Yang, and D. Li, "Restoration of interdependent network against cascading overload failure," *Phys. A, Stat. Mech. Appl.*, vol. 514, pp. 884–891, Jan. 2019.
[37] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, "Attack vulnerability of complex networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 65, no. 5, p. 56109, May 2002.
[38] P. Crucitti, V. Latora, M. Marchiori, and A. Rapisarda, "Error and attack tolerance of complex networks," *Phys. A, Stat. Mech. Appl.*, vol. 340, 1-3, pp. 388–394, Sep. 2004.
[39] C. M. Rocco, J. E. Ramirez-Marquez, D. E. Salazar, and C. Yajure, "Assessing the vulnerability of a power system through a multiple objective contingency screening approach," *IEEE Trans. Rel.*, vol. 60, no. 2, pp. 394–403, Jun. 2011.
[40] S. Iyer, T. Killingback, B. Sundaram, and Z. Wang, "Attack robustness and centrality of complex networks," *PLoS ONE*, vol. 8, no. 4, 2013, Art. no. e59613.
[41] S. Goyal and A. Vigier, "Attack, defence, and contagion in networks," *Rev. Econ. Stud.*, vol. 81, no. 4, pp. 1518–1542, Oct. 2014.
[42] S. Scellato, I. Leontiadis, C. Mascolo, P. Basu, and M. Zafer, "Understanding robustness of mobile networks through temporal network measures," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1–5.
[43] S. Trajanovski, S. Scellato, and I. Leontiadis, "Error and attack vulnerability of temporal networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 85, no. 6, p. 66105, Jun. 2012.
[44] S. Scellato, I. Leontiadis, C. Mascolo, P. Basu, and M. Zafer, "Evaluating temporal robustness of mobile networks," *IEEE Trans. Mobile Comput.*, vol. 12, no. 1, pp. 105–117, Jan. 2013.
[45] S. Sur, N. Ganguly, and A. Mukherjee, "Attack tolerance of correlated time-varying social networks with well-defined communities," *Phys. A, Stat. Mech. Appl.*, vol. 420, pp. 98–107, Feb. 2015.
[46] H. Feng, C. Li, and Y. Xu, "Invulnerability analysis of vehicular ad hoc networks based on temporal networks," in *Proc. 2nd IEEE Int. Conf. Comput. Commun. (ICCC)*, Oct. 2016, pp. 2198–2202.
[47] M. J. Williams and M. Musolesi, "Spatio-temporal networks: Reachability, centrality and robustness," *Roy. Soc. Open Sci.*, vol. 3, no. 6, Jun. 2016, Art. no. 160196.
[48] L. Lü, D. Chen, X.-L. Ren, Q.-M. Zhang, Y.-C. Zhang, and T. Zhou, "Vital nodes identification in complex networks," *Phys. Rep.*, vol. 650, pp. 1–63, Sep. 2016.
[49] J. Zhong, F. Zhang, and Z. Li, "Identification of vital nodes in complex network via belief propagation and node reinsertion," *IEEE Access*, vol. 6, pp. 29200–29210, 2018.
[50] I. Sutton, "Reliability, availability, and maintainability," in *Process Risk and Reliability Management*, I. S. Sutton, Ed. Amsterdam, The Netherlands: Elsevier, 2015, pp. 667–688.
[51] D. Li, Q. Zhang, E. Zio, S. Havlin, and R. Kang, "Network reliability analysis based on percolation theory," *Rel. Eng. Syst. Saf.*, vol. 142, pp. 556–562, Oct. 2015.
[52] D. Li, B. Fu, Y. Wang, G. Lu, Y. Berezin, H. E. Stanley, and S. Havlin, "Percolation transition in dynamical traffic network with evolving critical bottlenecks," *Proc. Nat. Acad. Sci. USA*, vol. 112, no. 3, pp. 669–672, Jan. 2015.
[53] F. Peruani, J. Starruß, V. Jakovljevic, L. Søgaard-Andersen, A. Deutsch, and M. Bär, "Collective motion and nonequilibrium cluster formation in colonies of gliding bacteria," *Phys. Rev. Lett.*, vol. 108, no. 9, p. 98102, Feb. 2012.
[54] M. Romenskyy and V. Lobaskin, "Statistical properties of swarms of self-propelled particles with repulsions across the order-disorder transition," *Eur. Phys. J. B*, vol. 86, no. 3, p. 99, Mar. 2013.
[55] V. Lobaskin and M. Romenskyy, "Collective dynamics in systems of active Brownian particles with dissipative interactions," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 87, no. 5, p. 52135, May 2013.
[56] A. Czirók and T. Vicsek, "Collective motion," in *Statistical Mechanics of Biocomplexity* (Lecture Notes in Physics), D. Reguera, J. M. G. Vilar, and J. M. Rubí, Eds., Berlin, Germany: Springer, 1999, pp. 152–164.



KANGKAI LIU received the B.S. degree from the School of Reliability and Systems Engineering, Beihang University, Beijing, China, in 2018, where he is currently pursuing the M.S. degree.

His research interests include complex networks, computer networks, and reliability engineering.



JILONG ZHONG received the Ph.D. degree from the Equipment Management and Safety Engineering College, Air Force Engineering University, and the School of Reliability and Systems Engineering, Beihang University, Beijing, China, in 2019.

He is currently an Assistant Research Fellow with the National Institute of Defense Technology Innovation, PLA Academy of Military Science, China. His current research interests include complex networks, reliability engineering, and artificial intelligence.

GUANGHAN BAI received the B.Sc. and M.Sc. degrees from the National University of Defense Technology, Changsha, China, and the Ph.D. degree in mechanical engineering from the University of Alberta, Edmonton, AB, Canada, in 2016.

He is currently a Lecturer with the Laboratory of Science and Technology on Integrated Logistics Support, National University of Defense Technology. His research interests include network reliability and system resilience.

YI YANG was born in 1978. She received the Ph.D. degree from the Nanjing University of Science and Technology, in 2008.

She was engaged in postdoctoral research with the School of Reliability and Systems Engineering, Beihang University (BUAA), where she has been a Professor, since 2019. Her main research interests include reliability analysis and design, traffic networks, control science and engineering, CPS, and belief reliability.