Toward Robust and Intelligent Drone Swarm: Challenges and Future Directions

Wu Chen, Jiajia Liu, Hongzhi Guo, and Nei Kato

Abstract

The rapid development of Space-Air-Ground integrated network, IoT, and swarm-based robotic systems has promoted the transformation of traditional single drone toward drone swarm. Compared to the traditional single drone, drone swarm can collaboratively complete complex tasks with higher efficiency and lower cost, especially in harsh environments. Communication and networking techniques are essential to enabling collaborate information sharing, coordinating multiple drones, and achieving autonomous drone swarm. However, the traditional communication technologies on fixed networks or slowly moving networks cannot address the unique characteristics of drone swarm, such as high dynamic topology, intermittent links and capability constraints. Two kinds of networking techniques fit for different drone swarm tasks are investigated, and the performance indexes of several wireless technologies suitable for drone swarm are also analyzed. Considering that drone swarm would usually be deployed in dire circumstances and the network may get frequently partitioned, the robustness of drone swarm becomes crucial. Based on the Molloy-Reed criterion, a swarm intelligent robust solution for drone swarm is proposed by using the consensus method and grey prediction, which has advantages of small overhead and local information exchanging. The simulation results corroborate that the robustness to node failure of drone swarm can be effectively improved by the proposed method.

Introduction

The Space-Air-Ground integrated network is an integration of satellite system, aerial networks, and terrestrial communication [1]. As an important role in the Space-Air-Ground integrated network, the drone has some incomparable advantages compared to any other vehicle. For example, the covered communication area for executing the task can be very flexible, including some hostile environments threatened by nuclear, biological and chemical weapons. Furthermore, drones can also quickly deploy a communication network in the environment lacking communication facilities. The drone swarm has become the significant working style for drones, with the vast potential for future development in both civil and military fields [2], such as smart cities [3] and tactical edge networks [4]. Compared with single drone, the drone swarm executes the task more effectively and economically. With the development of lightweight electronics and sensors, the size of drones and their cost have been reduced, enabling swarms to consist of small drones.

Figure 1 is a typical application scenario of drone swarm. Drone swarm is released and distributed over the mission area [5]. Drones equipped with different sensors collect environment information in real time, subsequently consolidate and report information to the command center, so as to make commanders better gather the on-site information and take appropriate measures. The drone swarm featured with high degree of autonomy can also get out from the personnel control and complete the task autonomously through mutual cooperation. Another major advantage of drone swarm is considered as easily expanding the scalar to execute more complex tasks. By means of distributing tasks and loads to multiple individual drones, the drone swarm can execute tasks in parallel to reduce the execution time with better fault tolerance. The limited sizes of nodes make the drone swarm difficult to be detected, hence the drone swarm has high survivability in the tactical environment.

While drone swarm brings these advantages, it also raises some challenging issues that need to be addressed [6]. It is noted that the drone swarm must possess a reliable and effective communication network. However, it is hard to be realized in drone swarm. As opposed to general wireless communication networks, the network communication system of drone swarm lacks the unified network architecture. The network architecture of the drone swarm is related to the task and the autonomy of the drone [7]. It requires to choose network infrastructure or flying Ad Hoc network (FANET) according to the autonomous capacity of the drone and tasks [8]. The special dynamic topological characteristics of drone swarm have also been concerned [9]. The topology is usually related to tasks, and node motion occurs in three-dimensional space. The speed of node varies in a wider range, from stationary to up to 100 m/s. Drone is usually a small platform with limited energy, computing and storage capacity. These characteristics increase the difficulty of protocol design.

Moreover, many drone swarms adopt open wireless channels in the system, which exposes them to a series of serious network security issues. In recent years, many researchers have involved in the works about the security technology of the drone swarm network. However, some challenging problems remain to be addressed regarding the security of drone swarm, including lack of effective model for the security system of drone swarm network, lack of evaluation mechanism for node behavior, imperfect solution for packet drop attack, and lack of study for active routing protocol security, etc.

Digital Object Identifier:
10.1109/MNET.001.1900521

Wu Chen, Jiajia Liu (corresponding author), and Hongzhi Guo are with Northwestern Polytechnical University, P.R. China; Nei Kato is with Tohoku University.

0890-8044/20/$25.00 © 2020 IEEE

Each drone in the drone swarm is equipped with only some functional equipment or sensors. The information interaction requires the network of drone swarm to be fully connected, which is the prerequisite for completing the task correctly. However, the drone swarm suffers from generally complex, harsh and highly confrontational environments. It is more prone to failure for the small platform in drone swarm than traditional drone, which will lead to the unguaranteed fully connected network of drone swarm.

Among the above challenging problems, anti-failure robustness becomes the most challenging problem. The drone swarm performs tasks based on information sharing of the whole network, hence the robustness to make sure the full connection of network is crucial. Nowadays, the main solution of network robustness including robust routing and network reconfiguration. Robust routing strategy introduces redundant resources to compensate for node failure. Network reconfiguration aims to configure the network topology in order to minimize network degradation caused by node and link failure.

However, these methods are not suitable for drone swarm. The robust routing method cannot guarantee a fully connected network. The network reconfiguration solution requires the entire network topology, which will cause excessive flooding. However, the payload is important for small drones. Toward this end, a robust control method for drone swarm based on a combination of swarm intelligence and Molloy-Reed criterion of percolation theory is proposed. It has the advantage of requiring only local information interaction.

The remainder of this article is organized as follows. We first introduce networking and communication techniques for drone swarm. Then the proposed robust method is described. Following that we present the simulation results to verify the performance of our solution. Finally, we conclude the article.

Networking and Communications for Drone Swarm

The main idea of drone swarm is to perform tasks based on the information shared with each other. Therefore effective communication and network techniques are key requirements for drone swarms. In this section, we overview the attractive networking and communication techniques which guarantee reliable communications for drone swarm.

Networking Techniques for Drone Swarm

As mentioned above, the network of drone swarm can be divided into infrastructure-based and flying Ad Hoc network-based, according to the autonomous capacity of drone swarm and the way of executing tasks.

Infrastructure-based Architecture: In the infrastructure-based drone swarm, a ground or air control station is responsible for receiving and processing messages that are sent back by drones. Meanwhile, the station controls drones individually in the swarm [10]. The collective previous literature considers Ad Hoc structure as the default network structure for drone swarm. However, since the autonomous capacity of current drones could merely reach a semi-autonomous level, the drone swarm completes tasks only under the control of the central node. Some tasks are more appropriate to be executed with central node control such as fixed-point surveillance and manned-unmanned teaming. Infrastructure-based architecture is more suitable for such situations.

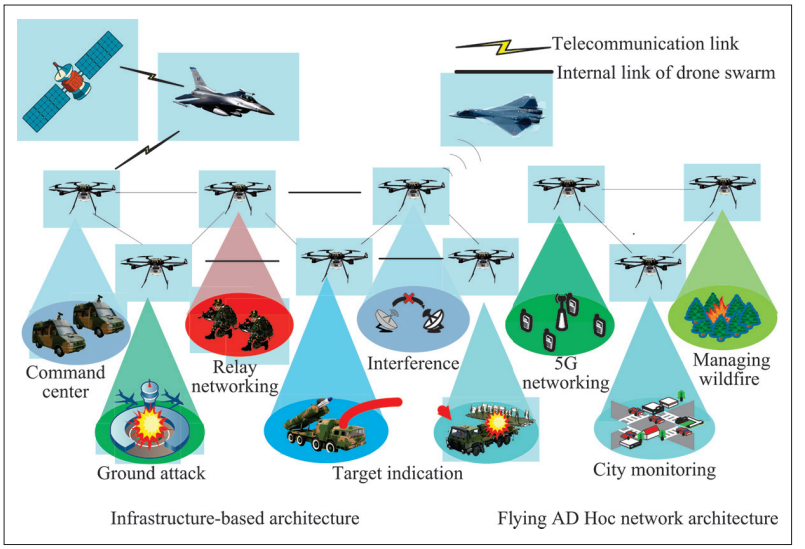

FIGURE 1. An application scenario of drone swarm.

In fact, the infrastructure-based architecture has been widely used in drone swarm, since the center node usually has strong computing ability and can command the drone swarm to complete significant complicated tasks. The response time for executing tasks is also short. Moreover, it is not required to establish a network connection between drones, hence the network protocol is simple and the networking is convenient. However, the infrastructure-based architecture relies on a central control node. This status decreases the network scalability. The scale of drone swarm is constrained by the processing capacity and the bandwidth of the control node. In addition, the failure of the central node leads to the collapse of the whole network and the low redundancy of the system. Since the central node directly controls drones, it requires the drone to remain in the wireless communication range of the central node, which limits the mission radius of drone swarm.

Flying Ad Hoc Network (FANET) Architecture: The network structure based on flying Ad Hoc network (FANET) architecture will be the mainstream network structure for future drone swarm [11], and also becomes the hotspot of current research. In this structure, central nodes will be negligible while the drones communicate with each other through mutual relay. Under the support of high-performance artificial intelligence algorithm, the drone will be more autonomous and not dependent on central nodes or human operators, but on sharing information between each other and accomplish the tasks together. In this case, drone swarms become fully autonomous application units which are suitable for dangerous applications.

Some other advantages of FANET are reminded: Under the FANET structure, nodes can join and leave the network dynamically, which increases the scalability of drone swarm. Even though some nodes fail, the remaining nodes can reconstitute the network through dynamic routing protocol, which improves the robustness of drone swarm. The emission power of the node will be reduced since

Features	Infrastructure-based Network	Flying Ad Hoc Network
Routing	Static Routing	Dynamic Routing
Representative Routing Protocol	LACD/DEQSPO/TBRPF	OLSR/AODV/MPCA/GPSR
Topology	Star	Mesh
Control	Centralized	Distributed
Commnication	Single-hop	Multi-hop
Scalablility	Low	High
Robust to Node Failure	Low	High
Control Complexity	Low	High
Autonomous Ability	Low	High
Cost of Control	Low	High
Bandwidth	High	Low
Latency	Low	High
Packct Loss	Low	High
Coverage	Small	Wide

TABLE 1. Comparison of networking techniques for drone swarm.

the mutual relay between each node. The possibility of drone swarm being detected can be further reduced, which improves the survivability of drone swarm in battlefield environment. However, obstacles of FANET structure are also obvious. The effective bandwidth of the network is reduced since all the nodes share the same channel. The cost of controlling will increase for maintaining the network, which also reduces the bandwidth of the system. In addition, the transmission delay in the network will occur due to multi-hop communication.

The comparisons between infrastructure-based and flying Ad Hoc network-based are shown in Table 1. Considering that the intelligence of the drone has not reached the completely autonomous level, some collaborative tasks can only be completed under personnel participation. The hybrid infrastructure/FANET network is suitable for such situations.

Communication Techniques for Drone Swarm

Despite different requirements for wireless communication techniques depending on its services, some common technical features can be provided including: moveable wireless devices, enough long communication distance between nodes, a sufficiently high data rate, minimized communication delay, supporting 3D movement, and slight influence from weather conditions. The mainstream wireless communication technologies meeting the aforementioned requirements, as well as their main features, are listed in Table 2.

IEEE 802.11: IEEE 802.11 series, collectively known as WiFi, involving the IEEE 802.11a/b/g/n standard, have become the most important wireless communication technique supporting Ad Hoc mode. IEEE 802.11 possesses higher bandwidth to guarantee the outside wireless communication range reaches to 150 m if the maximum speed reaches to 150 Mb/s. However, the maximum movement speed it supports is only 30 m/s, which also becomes the deficiency of the system. Consequently, it is not suitable for drone swarm network with high dynamic topology.

ZigBee: ZigBee, namely IEEE 802.15.4, is another wireless communication technique for Ad Hoc mode. ZigBee can support the large number of nodes with low energy consumption. The maximum communication range can also reach to 150 m. However, the data rate is only 250 kb/s which cannot support the drone swarm applications with monitoring type service.

WiMax: WiMax, which is the IEEE 802.16 standard, supports high data rate at a long distance such as 75 Mb/s data rate at a distance of 30 km. The characteristics of supporting nodes movement, strong anti-interference and easily arranging make WiMax appropriate for drone swarm communication. However, the latest frequency point of 802.16e needs to be applied for, which is one of the shortcomings of WiMax.

LTE: LTE has a higher transmission rate and supports wide bandwidth under high-speed mobile conditions with a delay of only 5 ms. These features are suitable for drone swarm executing surveillance operations. However, the usage of licensed band limits its application.

Currently, 5G is being deployed into commercial use. Drone swarm also plays an important role in 5G network, and it may have to deal with huge data flow with low latency. To meet this demand, some communication techniques are concerned for drone swarm such as millimeter-wave, nonorthogonal multiple access, and cognitive radio [12].

Robust and Intelligent Drone Swarm

The most attractive application scenario for drone swarm in the future is to execute tasks autonomously in harsh environments. Therefore, a high level of robust communication networks and intelligence are needed for drone swarm.

Fundamental Requirements for Drone Swarm

The robustness of drone swarms can be defined as the ability to complete missions after losing some drones or links. Compared to the traditional multi-function single platform drone like Reaper, the individual drone in the swarm is only equipped with some functional devices or sensors. Therefore, information sharing of the whole network is the prerequisite for drone swarm to execute collaborative tasks properly, which requires a fully connected network. Regarding the harsh and hostile environment the drone swarm works in, small drones that interact with each other over wireless channel with limited range are prone to fail than traditional aircraft. This situation results in the fully connected network of drone swarm not being guaranteed. A robust control method is needed, and the topology of the network can be adjusted to ensure the network fully connected when nodes or links are failure.

Combining Molloy-Reed criterion and swarm intelligence, a robust control method is proposed in this article to improve the robustness of the network by configuring the degree distribution of drones. Gray prediction is also introduced to achieve a fast estimation of the degree distribution of drones.

Molloy-Reed Based Solution

As a well known effective tool to determine the existence of a giant component [13], the Molloy-Reed criterion relies on a simple observation: for a network with a giant component, most nodes belonging to it must be connected to at least two other nodes. The starting point of the Molloy-Reed guidelines is that each node belonging to a giant component must be connected to two other nodes on average. Therefore, the average degree k_i for a randomly chosen node i, which is part of the giant component, should be at least 2. A variable κ is introduced in the Molloy-Reed criterion, equal to the average square degree divided by the average degree of the network.

Technologies	Standard	Data Rate	Device Mobility	Latency	Communication Range	Network Topology
802.11	802.11a	54 Mbps	Yes	Low	120 m	Ad Hoc/Star
	802.11b	11 Mbps	Yes	Low	140 m	Ad Hoc/Star
	802.11g	54 Mbps	Yes	Low	140 m	Ad Hoc/Star
	802.11n	600 Mbps	Yes	Low	250 m	Ad Hoc/Star
Zigbee	802.15.4	250 kbps	Yes	High	100 m	Ad Hoc/Star
WiMax	802.16a	75 Mbps	Yes	Low	48 km	Mesh
LTE	LTE	300 Mbps	Yes	Low	107 km	Mesh

TABLE 2. Comparison of communication techniques for drone swarm.

It can deduce that a network has a giant component if $\kappa > 2$ and the swarm is interoperable. The main idea of our method is to ensure the robustness of the drone swarm by reasonably configuring the link quality of the nodes, and configuring the degree distribution of the nodes to ensure $\kappa > 2$ as well.

On the basis of the Molloy-Reed criterion, the drone swarm robust control is achieved by the following steps.

Step 1: Obtaining the degree distribution of a drone. The degree distribution of a drone is determined by the link availability of the drone's edges. The link quality should be evaluated within a short time period while it is affected by many different factors. The GM(1,1) model in gray prediction can be taken into account to estimate the link quality with small samples, poor information and uncertain systems. Only four data items are required in GM(1,1). In this article, GM(1,1) model is adopted to get link availability of drones. The LQI/RSSI value is chosen as link quality evaluation criterion.

Step 2: Obtaining the average degree and average square degree of the whole network to calculate κ. The average degree of the whole network is represented by the mean value of the average degree of all nodes in the network. The average square degree of the whole network can be calculated similarly. In the average consensus, each drone obtains the degree distribution and broadcasts it to its neighbors. The drones find the average value of all the neighbor's degree distributions. This average degree is considered as the degree distribution of the whole network. The square degree distribution of the whole network can also be obtained by using the same method. It indicates that we can cast the degree distribution and the square degree distribution of the network by local information exchanging.

Step 3: Calculating κ when the drone obtains the value of the degree distribution and square degree distribution of the network. The robust control is implemented by adjusting the drone's transmitting power. $\kappa < 2$ means the network will break into many disconnected components, as a result, increasing the transmitting power is of significance for the drone. On the contrary, if $\kappa > 6$, the drone decreases its transmitting power to maintain κ between 2 and 6 for saving energy and reducing the probability of being discovered.

Furthermore, almost all route protocols are able to find the best route depending on the well-defined metric calculation algorithm. Since the nodes with the largest degree are susceptible to be selected, some central nodes in the network will be indispensable. Since the failure of central nodes will reduce network connectivity, it is crucial to avoid emergence of central nodes in the route selecting algorithm. Introducing betweeness to the cost function of the route protocol will solve this problem effectively.

Input: SNR/RSSI of drone's link.
Ouput: transmit power of the drone.
1: Initialization: $\kappa\_limit\_low = 2$;
2: Initialization: $\kappa\_limit\_up = 6$ *power_limit* $= P$;
3: **for** each node i and every time slot k in parallel **do**
4: Sample the link quality of all the links of the drone;
5: Predict the link quality at time $k + 1$ using grey prediction method;
6: Calculate the probability of the link at time $k + 1$;
7: Calculate degree distribution and square degree distribution at time $k + 1$ for each drone;
8: Broadcast degree distribution to its one hop neighbor nodes, and collect the degree distribution information of its neighbors;
9: Calculate the value of degree distribution and square degree distribution for each node of the network using average consensus method and get κ at time $k + 1$;
10: **if** self $\kappa < \kappa\_limit\_low$ and power $< P$ **then**
11: increase power of node;
12: **end if**
13: **if** power $> P$ or self $\kappa > \kappa\_limit\_up$ **then**
14: decrease power of node;
15: **end if**
16: **end for**

ALGORITHM 1. Robust algorithm based on Molloy-Reed criterion.

The aforementioned process can be summarized in Algorithm 1.

Challenges and Discussions

The main contribution of this article is to solve the two challenging issues by implementing the Molloy-Reed criterion in drone swarm. The first one is to calculate the whole network distribution through local information exchange. According to the Molloy-Reed criterion, calculating κ requires the degree distribution and the square degree distribution of each node in the whole network. However, considering the flooding in the whole network, it requires calculating the average degree of the whole network only by exchanging information between neighbor drones. The second one is to quickly evaluate link quality. The link quality is affected by various factors since drone swarm works in hostile environment. The long settling time cannot meet the requirement of the drone swarm to complete a task in a limited time period. Hence, an algorithm that can fast evaluate link quality in a small sample situation is desired.

In this article, the gray prediction method is adopted to quickly predict the link quality, as long as at least four samples exist. On this basis, the fast estimation for the degree distribution of the node itself can be realized. By using the average consistency algorithm in the multi-agent consistency method, the degree distribution of the whole network is estimated through local information interaction and sharing. Based on the estimated value, the node can autonomously regulate the power by

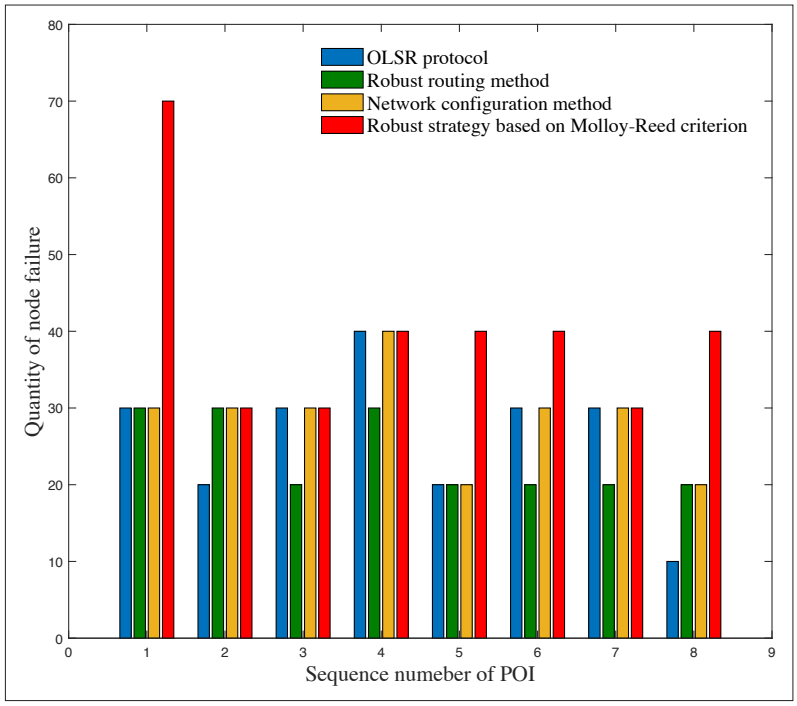

FIGURE 2. The quantity of removed nodes corresponding to the flow breakage. The greater value indicates the flow can tolerate more node failure.

using the Molloy-Reed criterion, thus the network robustness control could be implemented.

This proposed solution is essentially a small overhead swarm intelligence algorithm, which utilizes the mutual cooperation between nodes to achieve the network robust control. It avoids to demand high computational and storage capabilities of the nodes, making it an appropriate method for drone swarm applications. Since the distributed loads are adopted by the drone swarm, some of the nodes are equipped with higher performance loads to undertake more important tasks. These nodes are essential for drone swarm. Losing these nodes will incapacitate the drone swarm to execute tasks. Therefore, a protection solution for important nodes should be conducted in subsequent work.

Experimental Results

In order to evaluate the performance of our proposed robust method for drone swarm, we present some numerical results in this section.

Simulation Settings

The drone swarm simulation scenario of 'Grey Partridge' which consists of 103 nodes is established by Qualnet 5.0. The simulated scenario area is 1500 m by 1500 m. Drones are scattered randomly. The parameters of the simulation are chosen as MAC of 802.11, bandwidth of 6 Mb/s, initial power of 4 dBm and packet reception model of PHY 802.11a. Each node in the scenario moves in circle with random radius and spiral speed. The POI (Poisson) flows will send data messages with fixed size at time intervals satisfying Poisson distribution. Eight POI service flows are totally added to simulate the interaction between drones, in which six POI service flows are utilized to simulate communications between remote drones, and another two POI service flows are utilized to simulate communication between drones nearby. The comparisons of the proposed method with the standard OLSR routing protocol, the robust routing protocol with the betweeness cost function and the robust control of the network reconfiguration, are shown in the simulation scenes. The robustness to node failure is evaluated.

Numerical Results

We simulate the network being attacked by removing nodes randomly from the network. Ten nodes are removed randomly each time. The efficiency of the proposed algorithm is verified by observing the quantity of removed nodes corresponding to the breakage of eight POI data flows. Figure 2 shows the quantity of the failure nodes for different POI data flow breakages. As can be seen from the figure, the proposed method has significant advantage. For POI2, POI3 and POI7, the simulation results of the proposed method are similar to the robust routing method and network reconfiguration method, in which data flows will break when 30-40 nodes fail. For POI1, POI5, POI6 and POI8, the proposed method shows its advantage. Especially for POI1, the data flow still remains connecting when the failure nodes reach 70. It is due to the fact that for POI1, the route nodes are distributed in the center area of the network. The whole network information can be roundly obtained by sharing the node information, improving the efficiency of the proposed algorithm.

Despite of the data flow breakage, Fig. 3 shows the average packet loss rate versus the quantity of failure nodes, representing the average time delay of all data flows from POI1 to POI8 under node failure. As can be seen from the figure, for the robust routing method and network reconfiguration method, although portions of data flow remain connecting when the failure nodes reach 30-40, the packet loss rate has increased to around 90 percent and the data flow cannot support normal operation. But the packet loss rate of the proposed method is much less than the results of the robust routing method and network reconfiguration method, only 60 percent. It can be concluded that the proposed method shows better robustness.

Theoretically, introducing the betweenness to the cost function of the routing protocol avoids the occurrence of central node, thus improving the robustness of the drone swarm. However, the simulation results show that this method will be inefficient when faced with random attacks. Network reconfiguration method improves robustness by increasing the power of the most vulnerable nodes in the network, which is similar to the method proposed in this article, but the performance is not satisfactory as well.

Discussions

The proposed algorithm may cause slight delay jitter that is led by route change. It is a purely distributed swarm intelligent algorithm with great advantage to resist random attacks. The algorithm also improves network security. In general, network robustness solutions include robust routing and network reconfiguration as well [14]. The robust routing solution fails to effectively improve the robustness of node failure. The network reconfiguration solution requires the whole network topology. These become obvious drawbacks of the solutions to be applied in drone swarm.

The algorithm in this article is mainly aimed at the drone swarm of FANET structure. In the aspect of other networking and communication techniques like hybrid-structure and 5G communication, the robustness is mainly concerned with how to improve the robustness of edge gateway nodes and communication [15]. A solution combining centralized control and distributed control can be adopted in the proposed algorithm to improve the robust control effect. The performance of the network robustness can be greatly improved by introducing the small overhead intelligent algorithm to evaluate the importance of tasks and nodes. Evaluating algorithm will also become a significant research direction of drone swarm. It should be pointed out that the ability of nodes in the drone swarm is limited and only local information is collected. As a result, the swarm intelligent algorithm shows more advantages in drone swarm.

Conclusion

This article investigated the networking and communication techniques toward robust and intelligent drone swarm. In particular, we first analyzed the robust issues of drone swarm and presented our problem definition. After that, we proposed a robust control method based on the Molloy-Reed criterion which combines swarm intelligence and the grey prediction. Finally, a 'Grey Partridge' experimental scenario was established to construct the simulation. The experimental results validated that our proposed method, which performs robust control distributed and autonomous, can develop the reliability of data transmission and improve the robustness of the drone swarm network.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (61771374, 61771373, 61801360, and 61601357), and in part by the Fundamental Research Fund for the Central Universities (3102019PY005, and 310201905200001).

References

[1] J. Liu *et al.*, "Space-Air-Ground Integrated Network: A Survey," *IEEE Commun. Surveys & Tutorials*, vol. 20, no. 4, Fourth Qtr. 2018, pp. 2714–41.
[2] I. Bisio *et al.*, "Blind Detection: Advanced Techniques for WiFi-Based Drone Surveillance," *IEEE Trans. Vehicular Technology*, vol. 68, no. 1, May. 2019, pp. 938–46.
[3] F. Qi *et al.*, "UAV Network and IoT in the Sky for Future Smart Cities," *IEEE Network*, vol. 33, no. 2, Mar. 2019, pp. 96–101.
[4] M. Tortonesi *et al.*, "Multiple-UAV Coordination and Communications in Tactical Edge Networks," *IEEE Commun. Mag.*, vol. 50, no. 10, Oct. 2012, pp. 48–55.
[5] Z. R. Bogdanowicz, "Flying Swarm of Drones over Circulant Digraph," *IEEE Trans. Aerospace and Electronic Systems*, vol. 53, no. 6, Dec. 2017, pp. 2662–70.
[6] W. Shi *et al.*, "Drone Assisted Vehicular Networks: Architecture, Challenges and Opportunities," *IEEE Network*, vol. 32, no. 3, May 2018, pp. 130–37.
[7] L. Xiao *et al.*, "Security in Mobile Edge Caching with Reinforcement Learning," *IEEE Wireless Commun.*, vol. 25, no. 3, June 2018, pp. 116–22.
[8] Z. M. Fadlullah *et al.*, "A Dynamic Trajectory Control Algorithm for Improving the Communication Throughput and Delay in UAV-aided Networks," *IEEE Network*, vol. 30, no. 1, Jan. 2016, pp. 100–05.
[9] S. Park *et al.*, "DroneNetX: Network Reconstruction Through Connectivity Probing and Relay Deployment by Multiple UAVs in Ad Hoc Networks," *IEEE Trans. Vehicular Technology*, vol. 67, no. 11, Nov. 2018, pp. 11 192–11 207.
[10] Z. Zheng, A. K. Sangaiah, and T. Wang, "Adaptive Communication Protocols in Flying Ad Hoc Network," *IEEE Commun. Mag.*, vol. 56, no. 1, Jan. 2018, pp. 136–42.
[11] H. Khelifi *et al.*, "Bringing Deep Learning at the Edge of Information-Centric Internet of Things," *IEEE Commun. Lett.*, vol. 23, no. 1, Jan. 2019, pp. 52–55.

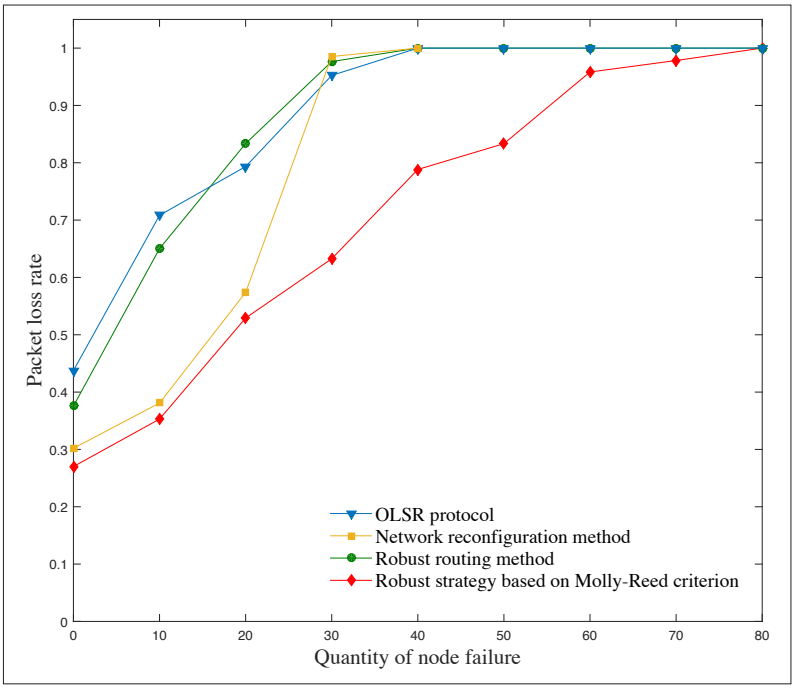

FIGURE 3. Packet loss rate when node failure increases gradually.

[12] B. Li, Z. Fei, and Y. Zhang, "UAV Communications for 5G and Beyond: Recent Advances and Future Trends," *IEEE Internet of Things J.*, vol. 6, no. 2, Apr. 2019, pp. 2241–63.
[13] A. L. Barabási, *Network Science*, Cambridge University Press, 2016.
[14] S. Sekander, H. Tabassum, and E. Hossain, "Multi-Tier Drone Architecture for 5G/B5G Cellular Networks: Challenges, Trends, and Prospects," *IEEE Commun. Mag.*, vol. 56, no. 3, Mar. 2018, pp. 96–103.
[15] H. Guo *et al.*, "Mobile-Edge Computation Offloading for Ultradense IoT Networks," *IEEE Internet of Things J.*, vol. 5, no. 6, Dec. 2018, pp. 4977–88.

Biographies

Wu Chen received the B.S. and M.S. degrees in navigation guidance and control from Northwestern Polytechnical University, China, in 1992 and 1997. He also received the Ph.D. degree in control theory and control engineering from Northwestern Polytechnical University, in 2000. Currently, he is an associate professor in the School of Cybersecurity, Northwestern Polytechnical University, China. His main research interests include Ad Hoc network, intelligent control, embedded system technology and information security.

Jiajia Liu [S'11, M'12, SM'15] is currently a full professor with the School of Cybersecurity, Northwestern Polytechnical University. His research interests cover wireless mobile communications, FiWi, IoT, etc. He has published more than 130 peer-reviewed papers in many prestigious IEEE journals and conferences, and currently serves as an editor for *IEEE Network*, TWC, TVT, and TCCN, guest editor for *IEEE IoT Journal* and TETC. He is a Distinguished Lecturer of IEEE ComSoc.

Hongzhi Guo [S'07, M'16] received his B.S., M.S., and Ph.D. degrees in computer science and technology from Harbin Institute of Technology in 2004, 2006, and 2011, respectively. He is currently an associate professor with the School of Cybersecurity, Northwestern Polytechnical University. His research interests cover a wide range of areas including MEC, AI, FiWi, IoT, 5G, smart grid, etc. He has published more than 30 peer-reviewed papers in many prestigious IEEE journals and conferences, and currently serves as an editor for the *International Journal of Multimedia Intelligence and Security*.

Nei Kato [A'03, M'04, SM'05, F'13] is currently a full professor at GSIS, Tohoku University. He currently serves as the Vice-President–Member & Global Activities of IEEE ComSoc, Editor-in-Chief of *IEEE Transactions on Vehicular Technology*, and Associate Editor-in-Chief of the *IEEE Internet of Things Journal*. He has also served as the Chair of the SSC and AHSN Technical Committees of IEEE ComSoc. He is a Distinguished Lecturer of IEEE ComSoc and the Vehicular Technology Society. He is a fellow of The Engineering Academy of Japan and IEICE.