Robustness Analysis of Flight Conflict Networks Based on Degree Correlation

FUGEN LIN1, XIANGXI WEN1,2, MINGGONG WU1,2, AND YUMING HENG1

1Air Traffic Control and Navigation College, Air Force Engineering University, Xi’an 710051, China
2National Key Laboratory of Air Traffic Collision Prevention, Xi’an 710051, China

Corresponding author: Xiangxi Wen (wxxajy@163.com)

This work was supported by the National Natural Science Foundation of China under Grant 71801221 and Grant 52074309.

ABSTRACT

Analyzing the composition and robustness of flight conflicts is beneficial to find the vulnerable sources of conflicts and dissipate flight conflicts, and effectively improve the safety and operational efficiency of air traffic. Therefore, this paper proposes a flight conflict network robustness evaluation method based on degree correlation. Firstly, a flight conflict network is constructed by using the velocity obstacle method, and it is classified into three types of assortative, disassortative and neutral conflict networks according to the degree correlation of the network. Several common robustness metrics in complex networks are explored, and a comprehensive robustness metric is proposed. The relationship between degree correlation and robustness of conflict networks under different node removal methods is analyzed by simulation experiments. The results show that the false alarm rate of the flight conflict network is decreased by 37.5% compared with the traditional state network. The degree correlation of the flight conflict network is closely related to the robustness. The assortative and disassortative conflict networks demonstrate stronger vulnerability with degree and betweenness removal, respectively, and the stronger the correlation the more obvious the vulnerability. The robustness of the neutral conflict network does not differ significantly under the two removal methods. Compared with random deletion, target removal can significantly decrease the network robustness.

INDEX TERMS

Flight conflict, air traffic, complex networks, degree correlation, robustness.

I. INTRODUCTION

With the rapid development of aviation industry, the surge of flight volume has deepened the conflict between airspace resources and air traffic flow, resulting in increasing airspace complexity and flight conflicts. The formation of flight conflicts has its unique endogenous properties, and the analysis of its causes and robustness plays a key role in the prevention and resolution of conflicts, which is also a hot topic of research in the industry.

Mid-traffic situations essentially respond to complex relationships between airborne aircraft and aircraft, and complex networks are an effective way to describe various complex relationships. This method has been widely used in the fields of power grids, infrastructure, transportation systems, and manufacturing industries [1], [2]. In the aviation field, Wang et al. [3] collected radar data and constructed a network with aircraft as nodes and the proximity relationship between aircraft as connected edges, and analyzed the significance of degree, network efficiency, and network structure entropy in the constructed network. Wang Xinglong et al. [4], [5], [6] constructed the air traffic network based on the relationship between airports, airways and sectors, and systematically analyzed its destructiveness, toughness and resilience, etc. Wen et al. [7], [8] built the flight state network based on the position conflict relationship between aircraft as the basis of the connected edges between nodes, and analyzed the airspace complexity by node deletion, SVM, and other methods. The air traffic network constructed by the above scholars has certain advantages in analyzing the relationship between aircraft and the complexity of airspace. However, constructing a conflict network by relying only on aircraft position relationship will miss a lot of important information. Therefore, in this paper, based on our previous work [7],...
we introduce the information of aircraft’s position, speed and direction, and construct the conflict network based on the speed barrier method with aircraft as nodes and conflicts as connected edges.

Conflict networks have characteristics that are generally found in complex networks, and therefore can be characterized by means of complex networks. Newman [9] first proposed in 2002 that there is a certain degree matching pattern between complex network nodes, and using this pattern can better understand and analyze the characteristics of complex networks. In the field of aviation, there are fewer studies based on network degree correlation, but there are a large number of studies in other fields that are worthy of reference: Kai Mao [10] used the degree correlation property to classify complex networks into three types and explored the stability and robustness of complex networks using variable gradient analysis; Wang et al. [11] analyzed the variation of the basic regeneration number R-0 of SIR epidemics in degree correlation networks. Mou et al. [12] provided theoretical references for port planning and national bulk trade strategies by analyzing trade networks with different degree correlation characteristics; Lu and Zhang [13] identified key nodes in complex networks by constructing similarity coefficients; Zhao et al. [14] classified the dependent networks into heterogeneous, homogeneous and random dependent ways according to the degree value of nodes and then analyzed the network robustness. Few of the above studies have analyzed degree correlation networks with different strengths or weaknesses, and have not clarified the changes in robustness of networks with different degree matching types after being subjected to deliberate and random attacks.

Flight conflict network robustness reflects the ease of controllers’ command deployment conflicts, which is explored in this paper by means of complex network robustness analysis. Typically, methods to assess the robustness of complex networks mainly consider random or deliberate attacks on the network structure and complex networks with cascading failures. In analyzing the robustness of complex networks, scholars have come up with rich results: Wang and Xia [15] found that the optimal attack strategy changes with different cost functions and attack methods considering the cost of the attack. Ratnayake et al. [16] proposed to evaluate the robustness of complex networks considering not only the topology but also the fitness function and fitness distribution among nodes. Many scholars have proposed some robustness metrics for specific systems. That is, robustness evaluation strategies are used to analyze the changes of individual parameters after node removal, such as the maximum connected subgraph, network efficiency, and average path length [17], [18]. These single robustness network characteristics metrics reflect only partial information and are not applicable to all complex network systems.

In summary, based on the existing research, we consider the degree-related characteristics of conflict network formation and classify them into three types of assortative, disassortative and neutral conflict networks, propose a general conflict network comprehensive robustness evaluation index, and explore the changes of the robustness index in the case of random and deliberate node deletion of the network to provide a reference basis for air traffic flight conflict command deployment.

The structure of this article is as follows, Section 1 of the article introduces the flight conflict network modeling method based on the speed barrier method. Section 2 illustrates the concept of degree correlation of the network, the measurement method and the conflict network degree correlation characteristics. Section 3 proposes a comprehensive robustness index and evaluation strategy for the conflict network. Section 4 conducts simulation experiments to analyze the relationship between degree correlation and robustness. Section 5 concludes the work of this paper and explains the shortcomings and outlook of the research.

II. FLIGHT CONFLICT NETWORK CONSTRUCTION

We construct a flight conflict network based on the conflicted relationship between aircraft to describe the air situation. Given \( G = (V, E, W) \), where \( V = \{v_1, v_2, v_3 \cdots v_n\} \) is the set of nodes in the network, i.e., aircraft, \( E = \{e_1, e_2, e_3 \cdots e_n\} \) is the set of connected edges in the network, \( W = \{w_1, w_2, w_3 \cdots w_n\} \) is the set of edge weights in the network, and the edge weights reflect the severity of the conflict.

A. FLIGHT CONFLICT NETWORK WITH EDGE DETERMINATION

Judgment of flight conflict is the key to determine the connected edge of flight conflict network. In the free flight state, according to the definition of aircraft protection zone, the horizontal distance of any two aircraft with the same flight altitude should not be less than 5 nautical miles (about 10km) and the vertical altitude should not be less than 2000 feet (600m). Based on this criterion, the protected area of the aircraft can be set, such as cylindrical, ellipsoidal or spherical protected area [19]. As shown in Fig.1, we choose an ellipsoid as a protected area with a long-axis focal length of \( d_r = 10km \) and a short-axis focal length of \( d_l = 600m \), and a conflict occurs when an aircraft protected area is invaded by other aircraft.

![FIGURE 1. Ellipsoid protection zone.](image-url)
Based on the protected area model, the conflict domain judgment equation \( C \) is constructed:

\[
C = \left\{ \frac{(x-x_c)^2}{d_c^2} + \frac{(y-y_c)^2}{d_c^2} + \frac{(z-z_c)^2}{d_l^2} \leq 1 \right\}
\]

where \((x, y, z)\) is the host coordinate, and \((x_c, y_c, z_c)\) is the potential conflict plane coordinate.

If the conflict situation is determined only based on whether the flight protection zone is invaded or not, ignoring important information such as heading and speed, it is easy to cause false alarms and cannot detect potential conflicts in time. As shown in Fig. 2, the arrow is the heading and the length of the arrow is proportional to the speed. In scenario 1, two aircraft are at the same altitude, and aircraft 2 invades the protected area of aircraft 1, which is judged to be in conflict. Similarly, in Scenario 2, the two aircraft are at different altitudes and within the ACAS communication response range (the distance between the two aircraft is less than 26 km). Because the protected area is not invaded, it will be judged as no conflict. In fact, there is a potential conflict between the two aircraft. Based on the above considerations, we were inspired by the research on obstacle avoidance in the field of robotics [20] and introduced the velocity barrier method to solve the problem based on the flight protection zone.

As shown in Fig. 3, if the flight direction \(\vec{v}_A, \vec{v}_B\) of two aircraft A and B is known, the tangent line (dotted line) of the ellipsoid is made over the point A, and B is taken as the reference, A makes relative motion. Use the vector triangle rule to determine the direction of their relative velocity \(\vec{v}_r = \vec{v}_A - \vec{v}_B\), the angle between \(\vec{v}_r\) and \(AB\) line is \(\alpha\), the angle between \(AB\) line and ellipsoid tangent line is \(\gamma\). \(\alpha\) and \(\gamma\) can be found from equations (2) and (3).

\[
\sin \alpha = \frac{d_l}{|AB|}
\]

\[\cos \gamma = \frac{\vec{v}_r \cdot AB}{|\vec{v}_r||AB|}
\]

\[|AB| = \sqrt{(x_A - x_B)^2 + (y_A - y_B)^2 + (z_A - z_B)^2}
\]

FIGURE 2. Conflict judgment scenarios.

FIGURE 3. Speed obstacle collision detection model.

As shown in Fig. 3, if the flight direction \(\vec{v}_A, \vec{v}_B\) of two aircraft A and B is known, the tangent line (dotted line) of the ellipsoid is made over the point A, and B is taken as the reference, A makes relative motion. Use the vector triangle rule to determine the direction of their relative velocity \(\vec{v}_r = \vec{v}_A - \vec{v}_B\), the angle between \(\vec{v}_r\) and \(AB\) line is \(\alpha\), the angle between \(AB\) line and ellipsoid tangent line is \(\gamma\). \(\alpha\) and \(\gamma\) can be found from equations (2) and (3).

\[
\sin \alpha = \frac{d_l}{|AB|}
\]

\[\cos \gamma = \frac{\vec{v}_r \cdot AB}{|\vec{v}_r||AB|}
\]

\[|AB| = \sqrt{(x_A - x_B)^2 + (y_A - y_B)^2 + (z_A - z_B)^2}
\]
From equation (7), it can be seen that the resolvable time \( T \) is inversely proportional to the relative velocity \( v_r \) and directly proportional to the intersection distance \( |AI_1| \) and \( |AI_2| \). The larger the relative velocity and the closer the distance, the less the resolvable time and the more urgent the conflict. Since the resolvable time is the opposite of the edge weight requirement, combined with the nature of the negative exponential function, the composite function is formed as shown in the following equation.

\[
\omega_{ij} = (e)^{-T}
\]

(8)

The edge weight \( \omega_{ij} \) is inversely proportional to the distance \( |AI_1|, |AI_2| \), and positively proportional to the velocity \( v_r \). The rate of change \( \omega_{ij} \) is larger as the resolvable time decreases, which can truly reflect the urgency of the conflict. Since the resolvable time \( T \) is positive, \( \omega_{ij} \) varies in the range of \([0,1]\) and plays a unitary role.

### III. DEGREE CORRELATION OF THE NETWORK

A large number of valuable research results have been obtained based on the degree correlation properties of networks \([10], [11], [12], [13], [14]\). In this section, by describing the degree correlation of complex networks and combining the composition characteristics of conflict networks, they are classified into assortative, disassortative and neutral conflict networks.

#### A. DEGREE CORRELATION OF COMPLEX NETWORKS

The formation of each complex network has certain structural characteristics, which are classified into Assortative Network (AN), Disassortative Network (DN), and Neutral Network (NN) from the perspective of network degree correlation. As shown in Figure 4(a), the hub nodes in AN tend to connect to each other rather than to the minor degree nodes, while the minor degree nodes tend to connect to each other in the minor degree nodes. As shown in Fig. 4(b), the hub nodes in DN tend to be not connected to each other but connected to the minor degree nodes. As shown in Figure 4(c), the node connections in NN are random, and the connection patterns between degrees are not correlated.

![FIGURE 4. Degree correlation network schematic.](image)

In order to quantitatively describe the degree-degree correlation of the network, Newman [9] obtained two degree sequences by traversing all links in the network, recording the degree values at both ends of each connected edge and then performing pearson correlation analysis on the degree sequences to obtain the degree correlation of the network.

Based on this, the degree correlation coefficient \( r \) can be used to describe the degree and degree correlation in the network.

\[
r = \frac{M^{-1} \sum_{e_{ij} \in E} k_i k_j - (M^{-1} \sum_{e_{ij} \in E} \frac{1}{2}(k_i + k_j))^2}{M^{-1} \sum_{e_{ij} \in E} k_i^2 + k_j^2 - (M^{-1} \sum_{e_{ij} \in E} \frac{1}{2}(k_i + k_j))^2}
\]

(9)

where \( k_i, k_j \) are the degrees of the nodes at the ends of the connected edges \( e_{ij} \). \( M \) is the total number of links in the network. \( E \) is the set of connected edges in the network.

The degree correlation coefficient takes the value of \(-1 \leq r \leq 1\). When \( r > 0 \), the degree of the network shows positive correlation, i.e., it is a assortative network; when \( r < 0 \), the degree of the network shows negative correlation, i.e., it is a disassortative network; when \( r = 0 \), the degree of the network has no obvious correlation characteristics, i.e., it is a neutral network.

#### B. DEGREE CORRELATION OF CONFLICT NETWORKS

The nodes and edges in general complex networks have abstract meaning, and changing the position of the nodes does not affect the network as a whole as long as the edges are kept intact. In contrast, the conflict network differs from the general complex network in that its nodes have Euclidean spatial location characteristics, and the node location distribution directly affects the topology of the network. Therefore, based on the description of degree correlation in the previous section, the change of \( r \)-value can visually express the formation characteristics of conflict. As shown in Figs. 5(a) and 5(b), the former is the assortative conflict network \( r \approx 0.4 \) and the latter is the disassortative conflict network \( r \approx -0.4 \). It can be seen that when the conflict network is congruent, the aircraft with more conflicts gather together to reflect stronger local conflicts; while when the conflict network is heterogeneous, the aircraft with more conflicts (larger degree values) are spread all over the airspace connecting small degree nodes.

![FIGURE 5. Degree correlation of conflict networks.](image)

In analyzing the correlation coefficient, Buda Andrzej suggested in his work that the value of the correlation coefficient is related to the strength of its correlation \([21]\). Since the value of the degree correlation coefficient \( r \) is difficult to be taken precisely to a definite value. Therefore, we segment its value, and when \( 0.1 < r \leq 1 \) is called Assortative Conflict.
of the node strengths of all nodes. This value can reflect the urgency of the conflict situation and indirectly expresses the average pressure of control deployment, which is expressed by $\bar{S}$

$$\bar{S} = \frac{1}{N} \sum_{j=1}^{N} a_{ij} \omega_{ij}$$  (12)

where $\bar{S}$ is the average node strength, $a_{ij}$ denotes the connection relationship between nodes $i$ and $j$, if connected then $a_{ij} = 1$, otherwise $a_{ij} = 0$, $\omega_{ij}$ is the edge weight between nodes $i$ and $j$.

Definition 3: Network efficiency $E$

The network efficiency can visually reflect the connectivity of the whole network, and the efficiency between two nodes is expressed as the reciprocal of the distance between each other, while the efficiency of the whole network is the average of the efficiency between every two pairs of nodes. This value can easily represent the diffusion breadth of aircraft conflicts and grasp the conflict dynamics at a macro level, denoted by $E$.

$$E = \frac{1}{N(N-1)} \sum_{i \neq j} \frac{1}{d_{ij}}$$  (13)

where $d_{ij}$ is the shortest path between nodes $i$ and $j$.

Definition 4: Largest connected ratio $F$

In a conflict network, the ratio of the number of nodes belonging to the largest giant connected branch to the total number of nodes in the network is called the maximum connectivity ratio. This value reflects the overall postural complexity of the conflict and is denoted by $F$.

$$F = \frac{N'}{N}$$  (14)

where $N'$ is the number of nodes with giant connected branches, $N$ is the total number of nodes in the network.

For different flight conflict network structures, the variation of each metric value is different. In order to accurately and objectively define the comprehensive robustness evaluation metrics of the conflict network, we determine the weights of the four metrics set by performing sensitivity analysis on them. Generally, if a metric value changes significantly with them, generally, if a metric value changes significantly with the variation of the network, we will give it a larger weight because it reflects the change of the characteristics of the network well. The sensitivity analysis method is described as follows.

For a conflicting network consisting of $n$ nodes, the network nodes are removed in turn and the network feature metric is calculated. Then, a set of network feature variation values and the average network feature variation can be obtained. The variance of the metric changes can be calculated by the following equation.

$$S^2_k = \frac{\sum_{i=1}^{n} (\Delta s_{ki} - \bar{\Delta s}_k)^2}{n}$$  (15)
Then, repeating the above process \( N \) times, the mean value of the variance of the variance of the network characteristics is obtained, which can be expressed as

\[
\overline{S_k^2} = \frac{1}{N} \sum_{k=1}^{N} S_k^2
\]  

(16)

The value of \( \overline{S_k^2} \) is used to determine the weight of each metric in the comprehensive robustness metric, which is calculated as follows.

\[
\omega_k = \frac{S_k^2}{\sum_{k=1}^{p} S_k^2}
\]  

(17)

Finally, the comprehensive robustness metric \( R \) of the flight conflict network is obtained using the normalization method.

\[
R = \sum_{k=1}^{p} \omega_k \frac{s_k - \min(s_k)}{\max(s_k) - \min(s_k)}
\]  

(18)

where \( R \) denotes the robustness of the flight conflict network, and \( R \) takes values in the range of \([0, 1]\). The larger the number, the more robustness is indicated.

**B. ROBUSTNESS EVALUATION STRATEGY**

Node removal is an important evaluation method for network robustness assessment. Therefore, the selections of different node removal strategies can have a great impact on the evaluation results of conflict networks. Currently, there are two main types of node removal: random removal and targeted removal, i.e., random and targeted provisioning of conflicts.

The controllers will intentionally deploy some nodes in the flight conflict, and random deployments can be used as a control group to verify the effectiveness of targeted deployments. Therefore, when analyzing the robustness of conflict networks with different degrees of correlation, both random and targeted deployment should be considered. In targeted deployment, the aircraft (nodes) with more conflicts or that can break up the conflict network quickly are usually deployed in preference, i.e., remove node based on the highest degree or betweenness. According to the structure and functional characteristics of the flight conflict network, the robustness evaluation strategy selected in this study is as follows:

1) **RANDOM REMOVAL (RR)**

Simulation of random provisioning flight conflicts, i.e., random removal of nodes from the network for flight conflict networks without considering any attributes of the nodes.

2) **HIGHEST DEGREE REMOVAL (DR)**

Simulate the deployment of the aircraft with the most conflicting connected edges. The nodes with the highest node degree are first eliminated, and then the nodes in the conflicting network are removed in descending order of degree value (the degree value of a node is the number of connected edges of the node).

3) **HIGHEST BETWEENNESS REMOVAL (BR)**

Simulate the deployment of the most critical aircraft at the location of the conflict. The nodes in the conflict network are removed in the same way as the highest degree deployment, the nodes in the conflict network are removed in order from the largest to the smallest by the value of the betweenness. The betweenness is calculated as follows.

\[
B(i) = \sum_{1 \leq j \leq l \leq N, j \neq i \neq l} [n_{jl}(i)/n_{jl}]
\]  

(19)

where \( n_{jl} \) is the shortest path between node \( j \) and \( l \), \( n_{jl}(i) \) is the number of shortest paths between node \( j \) and \( l \) that pass through node \( i \).

The faster the robustness metric decreases after the conflict network is subjected to different strategies of deployment, the more effective the method is.

**C. ROBUSTNESS ANALYSIS PROCESS**

The method for robustness analysis of flight conflict networks based on degree correlation is shown in Fig. 6 in the following steps.

*Step 1:* The flight conflict network is constructed using the velocity obstacle method based on the information of aircraft’s speed, heading and location.

*Step 2:* Classify the conflict networks into three types according to the degree correlation coefficient \( r \), which are assortative, disassortative and neutral conflict networks.

*Step 3:* The comprehensive robustness metric \( R \) is established by sensitivity analysis using average weighted clustering coefficient, average node strength, network efficiency and largest connected ratio.

*Step 4:* The nodes in the network are removed by three strategies: degree removal, mediator removal and random removal, and the change in robustness of different types of conflicting networks is analyzed and conclusions are drawn accordingly.

**V. SIMULATION EXPERIMENTS AND ANALYSIS**

In Sections II-IV of this paper, we introduce the modeling approach for in-flight conflict networks, illustrate the properties of conflict network degree correlations, and propose a corresponding integrated robustness evaluation algorithm. In this section, we analyze the robustness of conflict networks with different degree correlations through simulation experiments.

**A. SIMULATION EXPERIMENT SETUP**

In this paper, a 300km*300km airspace is simulated by Matlab software, and 75 aircraft are randomly generated in the airspace. After generating the parameter information of aircraft nodes, we generate “ellipsoidal protection zone” for each node according to Section II of the paper, determine the conflicting edge relationship between nodes according to equations (1-6), and use equations (7-8) to determine the weight of connected edges, thus forming a conflict network.
After visualizing the network structure, as shown in Fig. 7, each node in the figure represents an aircraft, and the connected edges between the nodes represent the existence of conflicts between two aircraft. The thickness of the edges indicates the urgency of the conflict, and the size of the nodes increases with the increase of the number of conflicts, the larger the nodes and the darker the color represents the more conflicts.

**B. NETWORK PERFORMANCE**

The construction of flight conflict network is an accurate quantitative analysis of the air traffic situation, and the conflict network visualization facilitates to provide auxiliary decisions to controllers when targeting high complexity. As shown in Fig. 8, the flight state network constructed by our previous work [7] is based on the position relationship, as long as two aircraft nodes are less than 52km, it constitutes a conflict. Fig. 9 shows the conflict network constructed based on the speed barrier method in this paper. Comparing the nodes 1 and 2 in Fig. 8 and 9, the position distance between the nodes is greater than 52km, which does not constitute a conflict in the state network, while there is a potential conflict when considering the flight heading and speed of the two nodes, the conflict network identifies it and predicts the potential conflict in advance. In contrast, nodes 3 and 4 in the figure, the distance between the two nodes’ positions is less than 52km, which constitutes a conflict in the state network, but there is no conflict when considering the two nodes’ heading and speed.

Comparing the number of conflicting connected edges in Figs. 8 and 9, the connected edges of the state network are 45 and the conflicting network is 30, which reduces the false alarm rate by 33.3% compared to that. Since the decrease ratio of false alarm rate at a single moment is somewhat chance, we randomly generate 10-75 aircraft in the airspace for the false alarm rate comparison and repeat the experiment.
average clustering coefficient. Based on the method in Section 4, four metrics, namely, the reduces the false alarm rate by 37.5% on average. value is 37.5%, thus it is considered that the conflict model concentrated between 30% and 45%, and the overall average the outlier points. It can be seen that the data distribution is are the upper and lower limits of the points after removing black dots are the outlier points, and the vertical black lines is the nuclear density curve, the white squares are the 25%, the middle horizontal line is the median, the and the largest connected ratio F, of each metrics were measured as [0.1023,0.3944,0.2247,0.2786], respectively, and the generic comprehensive robustness metric R was obtained as shown in equation (20)

\[
R = \omega_1 \frac{C - \min(C)}{\max(C) - \min(C)} + \omega_2 \frac{S - \min(S)}{\max(S) - \min(S)} + \omega_3 \frac{E - \min(E)}{\max(E) - \min(E)} + \omega_4 \frac{F - \min(F)}{\max(F) - \min(F)}
\]  

(20)

According to the previous evaluation strategy for the robustness of conflicting networks, 30 networks with degree correlations r close to 0.5, 0 and −0.5 were selected and their nodes were subjected to Random Removal (RR), Degree Removal (DR) and Betweenness Removal (BR) in order to reduce randomness and contingency, and then their robustness was analyzed.

As shown in Fig. 11, the experimental results are the average values after 30 experiments, and the number of maximum deployed (y removed) aircraft is set to 40% of the total number of aircraft. Fig. 11(a) shows the robustness of the assortative conflict network with degree correlation r close to 0.5 under random removal and target removal, and it can be seen that the DR and BR approaches can steadily reduce the robustness of the network under the assortative conflict network, and the degree removal is better than the betweenness removal. Fig. 11(b) shows the robustness of the neutral conflict network with degree correlation r close to 0. In the neutral network, there is no significant difference between the DR and BR approaches for reducing the robustness of the conflict network, but both outperform RR. Fig. 11(c) shows the robustness of the disassortative conflict network with degree correlation r close to −0.5. In this case, the BR approach outperforms the DR approach, and both outperform random removal. The network robustness decreases gradually with target removal, while random removal shows a fluctuating decrease, indicating that target removal can significantly reduce the network robustness.

From the above analysis, when the conflict network is an assortative network, it is more beneficial to choose the aircraft with a higher degree value of deployment to dissipate the conflict. When the conflict network is a neutral network, there is no significant difference between the deployment of degree and the deployment of betweenness. When the conflict network is a disassortative network, the aircraft with a higher betweenness is more beneficial for conflict resolution. In the case of different types of degree correlations, both the degree and the betweenness-based deployment methods are better than random deployment.

To further analyze the relationship between the degree correlation and robustness of the flight conflict network. We control the value of to observe the variation of the robustness of the network under the degree deployment of the assortative conflict network and the betweenness deployment method of the disassortative conflict network.

For the assortative conflict network, we take 20 different networks with degree correlation r ≈ [0.2, 0.4, 0.6, 0.8] and remove node in the highest degree, respectively. The robustness metrics obtained each time are recorded, and finally the average value is taken as the experimental result.
FIGURE 11. Network Robustness with three different degree correlations.

FIGURE 12. ACN degree value deletion effect.

For random removal as a comparison test, the overall average is taken. Interestingly, as shown in Fig. 12, the robustness of the network decreases rather than increases as the degree correlation of the congruent conflict network increases, and the highest degree removal strategy is used to deploy the conflict more effectively, and both are better than random removal. After removing about 35% of the nodes, no significant difference is shown because the overall structure of the network is destroyed.

Similarly, as shown in Fig. 13, the experimental results of the disassortative conflict network taking $r \approx [-0.2, -0.4, -0.6, -0.8]$, after the removal by the betweenness. It can be seen that with the gradual increase of disassortative correlation, a weaker robustness is revealed under the betweenness removal, but the hierarchical effect of the removal is not as obvious as the degree removal of the assortative conflict network. Since the betweenness removal is more likely to destroy the overall structure of the network, the curves appear to intersect after about 25% of the nodes are removed. The target removal effect is significantly better than the random removal.

In summary, the robustness of the conflict network and the degree correlation of the network are closely related. When the degree assortative of the conflicting networks is enhanced, the better the degree deployment is selected.

When the degree disassortative of the conflicting networks increases, the choice of betweenness deployment can quickly reduce the robustness of the network. Meanwhile, networks with severe local conflicts (the higher $r$) are more vulnerable, and reducing the redundant connected edges of nodes with high degree values reduces the network robustness. The target deployment has a significant advantage over random deployment.

VI. CONCLUSION

In this study, a flight conflict network is constructed based on the velocity obstacle relationship between aircraft, and robustness analysis is performed for networks with different degree correlation, and the main conclusions obtained are as follows.

(1) The information of aircraft speed, heading and position is introduced, and a more reasonable conflict network is constructed by using the velocity obstacle method. Compared with the state network, the false alarm rate is decreased by 37.5%.

(2) The classification of conflict networks based on the degree correlation of complex networks reflects the topology of conflict formation objectively, which is beneficial to the analysis of conflict network characteristics.
(3) A comprehensive robustness metric for conflict networks was built based on four commonly used network topology metrics.

(4) The network robustness is analyzed by evaluating the random removal and target removal of network nodes, and it is found that the robustness of different types of networks with different degree correlation characteristics changes with the change of node removal strategies for decreasing the conflict network robustness. The highest removal method is better than the betweenness removal method for assortative conflict networks. The disassortative conflict network using the largest betweenness removal method is better than the largest degree removal method. The above effect is more obvious with the enhancement of the degree correlation property.

From the analysis of this paper, it can be seen that the degree correlation and robustness of flight conflict network are closely related, which can provide some theoretical reference for air traffic control command. However, there are more comprehensive factors to be considered when controllers deploy conflicts, and the conclusions of this paper need to be put into practical applications for verification, which is also an important direction for our subsequent research.

REFERENCES

[1] A. Fichera, M. Frasca, and R. Volpe, “Complex networks for the integration of distributed energy systems in urban areas,” Appl. Energy, vol. 193, pp. 336–345, May 2017.

[2] H. Yang and S. An, “Robustness evaluation for multi-subnet composited complex network of urban public transport,” Alexandria Eng. J., vol. 60, no. 2, pp. 2065–2074, Apr. 2021.

[3] W. Hongyong, W. Ruixing, and Z. Yifei, “Analysis of topological characteristics in air traffic situation networks,” Proc. Inst. Mech. Eng., G, J. Aerosp. Eng., vol. 229, no. 13, pp. 2497–2505, Nov. 2015.

[4] X. L. Wang and M. He, “Research on the influence node ordering and destructive resistance of air traffic cyber-physical system,” Acta NUAA China, vol. 38, no. 2, pp. 288–297, 2021.

[5] X. L. Wang, Z. B. Shi, and Z. Y. Chen, “Air traffic network modal identification and subgraph structural toughness assessment,” Acta Aeronaut. Astronaut. Sinica China, vol. 42, no. 7, pp. 558–568, 2021. [Online]. Available: https://kns.cnki.net/kcms/detail/11.1929.V.20201030.1637.022.html

[6] X. L. Wang and Y. Liu, “Aviation multilayer network resilience measurement and analysis,” Complex Syst. Complex. Sci. China, vol. 17, no. 2, pp. 31–38, 2020.

[7] X. X. Wen, C. L. Tu, and M. G. Wu, “Node importance evaluation in aviation network based on ‘no return’ node deletion method.” Phys. A, Stat. Mech. Appl., vol. 503, pp. 546–559, Aug. 2018.

[8] X.-R. Jiang, X.-X. Wen, M.-G. Wu, Z.-K. Wang, and X. Qiu, “A SVM approach of aircraft conflict detection in free flight,” J. Adv. Transp., vol. 2018, pp. 1–9, Dec. 2018.

[9] M. E. J. Newman, “Assortative mixing in networks,” Phys. Rev. Lett., vol. 89, no. 20, Oct. 2002, Art. no. 208701.

[10] K. Mao, “Research on stability and robustness of complex network structures,” J. Sci. China, vol. 42, no. 4, pp. 85–88, 2015.

[11] Y. Wang, J. Ma, and J. Cao, “Basic reproduction number for the SIR epidemic in degree correlated networks,” Phys. D, Nonlinear Phenomena, vol. 433, May 2022, Art. no. 133183.

[12] N. Mou, Y. Fang, T. Yang, and L. Zhang, “Assortative analysis of bulk trade complex network on maritime silk road,” IEEE Access, vol. 8, pp. 131928–131938, 2019.

[13] P. Lu and Z. Zhang, “Critical nodes identification in complex networks via similarity coefficient,” Mod. Phys. Lett. B, vol. 36, no. 9, Mar. 2022, Art. no. 2150620.

[14] N. Zhao, Y. M. Cai, C. L. Yi, Z. Yang, J. Wang, and S. Su, “Robustness analysis of coherent networks based on the relative effectiveness of maximum connected subgraphs,” J. Univ. Electron. Sci. Technol. China, vol. 50, no. 4, pp. 627–633, 2021.

[15] C. Wang and Y. Xia, “Robustness of complex networks considering attack cost,” IEEE Access, vol. 8, pp. 172398–172404, 2020.

[16] P. Rattanayake, S. Weragoda, J. Wansapura, D. Kathurirathana, and M. Piraveenan, “Quantifying the robustness of complex networks with heterogeneous nodes,” Mathematics, vol. 9, no. 21, p. 2769, Nov. 2021.

[17] X. Fen and H. C. Jia, “Robustness of aviation networks considering node failure and edge failure,” J. Beijing Jiaotong Univ. China, vol. 45, no. 5, pp. 94–92, 2021. [Online]. Available: https://kns.cnki.net/kcms/detail/11.5258.U.20211124.0940.020.html

[18] Y. Zhou and J. Wang, “Efficiency of complex networks under failures and attacks: A percolation approach,” Phys. A, Stat. Mech. Appl., vol. 512, pp. 658–664, Dec. 2018.

[19] E. Saluam, M. Garial, A. E. Vela, and E. Feron, “Aircraft proximity maps based on data-driven flow modeling,” J. Guid., Control, Dyn., vol. 35, no. 2, pp. 563–577, Mar. 2012.

[20] P. Fiorini and Z. Shiller, “Motion planning in dynamic environments using velocity obstacles,” Int. J. Robot. Res., vol. 17, no. 7, pp. 760–772, Jul. 1998, doi: 10.1080/02783649808928007.

[21] A. Buda and J. Andrzje, Life Time of Correlations and Its Applications. Warsaw, Poland: Wydawnictwo Naukowe, 2010, pp. 5–21.

[22] A. Li, D. M. Nie, X. X. Wen, B. H. Han, and Y. J. Zeng, “Evolutionary process of control-flight state dependence network,” Acta Aeronaut. Astronaut. Sinica China, vol. 42, no. 9, pp. 481–493, 2021. [Online]. Available: https://kns.cnki.net/kcms/detail/11.1929.V.202010204.1016.004.html

FUGEN LIN was born in 1997. He received the B.S. degree from Henan Polytechnic University, Jiaozuo, China, in 2020. He is currently pursuing the master’s degree with Air Force Engineering University. He is currently pursuing the degree with the School of management, Air Force Engineering University. His research interests include complex networks, air traffic control, and system modeling and simulation.

XIAOXI WEN received the B.S., M.S., and Ph.D. degrees from Air Force Engineering University. He has more than 30 articles and participated in a number of national topics. His research interests include aviation network security, complex network theory, and intelligent air traffic systems.

MINGGONG WU was born in 1966. He is currently a Professor of traffic and transportation engineering at Air Force Engineering University. His research interests include air traffic control operation and airspace management and air traffic control.

YUMING HENG was born in 1998. He received the Bachelor of Engineering degree from the Hefei University of Technology, in 2020. He is currently pursuing the master’s degree with Air Force Engineering University. His research interests include air traffic control, controller load, and complex networks.