



Research Article

Coupled-Map-Lattices-Based Vulnerability Assessment of UAV Network in Interference Scenarios

Xiaoyu Xie ¹, Jinglei Li,¹ Zijia Huang,² Qinghai Yang,¹ and Kyung Sup Kwak ³

¹School of Telecommunications Engineering, Xidian University, Xi'an 710071, China

²The 20th Research Institute of China Electronic Technology Group Corporation, Xi'an 710068, China

³Communication Engineering, Inha University, Incheon 402-751, Republic of Korea

Correspondence should be addressed to Xiaoyu Xie; h578960@163.com

Received 13 June 2022; Revised 26 September 2022; Accepted 6 October 2022; Published 21 October 2022

Academic Editor: Chi-Hua Chen

Copyright © 2022 Xiaoyu Xie et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

On the modern information battlefield, UAV have been widely used due to the advantages of no casualties and good maneuverability. However, during the UAV swarm combat, the UAV network will be interfered by the enemy, which will damage some key UAV nodes or communication links and affect the connectivity of the entire network, thus leading to the fact that the entire network becomes more vulnerable. Therefore, it is necessary to study the network vulnerability of UAV networks in interference scenarios. In this paper, a coupled map lattice (CML) model which is a dynamic system with discrete time, discrete space, and continuous state variables is proposed to assess the vulnerability of UAV networks. The CML model integrates multiple topological indicators such as node degree, node betweenness, and node clustering coefficient, and reflects the node state change of the UAV network in the interference scenario from the topological point of view. When changing the strategy of interfering UAV nodes in different interfering scenarios, the relative network efficiency and failure proportion are used as indicators to study the change of network vulnerability. The studies show that precisely interfering important UAV nodes in a network can cause more damage to the UAV network. We also discover that as the intensity of external interference increases, the entire network will become increasingly vulnerable and the vulnerability of the network will also have different manifestations under different interfering strategies.

1. Introduction

In recent years, UAVs have been widely used in the field of wireless communication due to their advantages of simple operation, flexible application, strong adaptability, and wide coverage. However, malicious attacks and electromagnetic interference from the enemy will block the communication channel of the UAVs, destroy the communication link of the UAV network, and even make the UAVs lose contact with the console. Therefore, stability and connectivity will be greatly affected. To protect some master control nodes and important communication links in the whole UAVs network, it is necessary to study the vulnerability of the network under different interference scenarios.

Network vulnerability analysis is a critical part of the overall network performance assessment. The research on network vulnerability and related assessment methods has

become a current research hotspot. The topology of a network is the most important of all factors that affect network vulnerability. For many years, people have been working on assessing the vulnerability of network topologies and finding effective algorithms to enhance the robustness of networks. Although predecessors have done some research on the vulnerability of the network, the evaluation indicators for the key nodes in the network topology are relatively single, and cannot comprehensively reflect the importance of the nodes in the network. Because of these deficiencies in the research, we analyze and study the network's vulnerability in terms of network topology.

When it comes to studying the change in the network vulnerability, cascading failure is another key research point that cannot be avoided. Researchers have found cascading failures in many important natural and man-made networks, including power networks and the Internet.

Cascading failure refers to the avalanche failure process caused by the initial disturbance in the complex network. Due to the coupling relationship between nodes, failures can continue to spread from a node to other nodes in the network through cascading, which may cause large-scale damage and serious economic losses.

In this paper, three different interference scenarios that UAV communication networks may encounter in practice are considered to analyze the vulnerability of the network. Aiming at the problem that the importance evaluation indicators in previous studies are relatively single, we use three commonly used node importance evaluation indicators as factors such as degree, betweenness, and clustering coefficient when constructing the model. Since the dynamic vulnerability of a network is difficult to measure, we use a discrete-time, discrete-space, and continuous-state coupled map lattice approach to identify cascading failures and assess the network's vulnerability. Based on coupled map lattices theory, an integrated cascading failure analysis model which evaluates key nodes and state changes from a topological perspective is proposed for exploration. Meanwhile, cascading failures are introduced in the in-depth analysis of network vulnerability in interference scenarios to observe the dynamic changes of the network when it has interfered.

The paper is organized as follows. In Section 3, we discuss the network topology index and evaluation index. Section 4 demonstrates the CML-based cascading failure model. In Section 5, simulation results and discussion are provided. Finally, the work is summarized in Section 6.

2. Literature Review

In recent years, more and more researchers have shown interest in the vulnerabilities of various networks. In this regard, most scholars' research focuses on the identification of key nodes. Wang et al. studied the vulnerability of urban rail transit networks based on graph and complex network theory [1–3]. Jing et al. proposed a method to identify key nodes and analyzed the vulnerability of Shanghai Metro [4]. Cats et al. analyzed the link capacity of the subway network based on complex network [5]. Liu and Song analyzed the distribution of Guangzhou rail transit network degree, clustering coefficient, and average shortest path [6]. Zhang et al. explored the topological characteristics of the Shanghai subway system and assessed the connectivity or reliability of the subway lines [7]. Hong et al. developed a method to analyze the vulnerability of urban public transport systems from the perspective of their common functions [8]. At the same time, there are many kinds of literature that study the structural characteristics and vulnerabilities of transportation networks [9–11]. Yang et al. proposed a new weighted composite index to evaluate node importance and study the topological properties of subway systems by evaluating their robustness in the face of random failures and malicious attacks [12]. Taking the Shanghai subway network as an example, Sun evaluates the vulnerability of the subway network from the perspective of line operation based on on-site passenger flow data [13]. Qiao et al. propose a key node identification algorithm based on multiattribute weighted

fusion. This algorithm can not only be used to identify the key nodes of different types of complex networks but also be easy to be extended [14].

In the research of cascading failures, many scholars at home and abroad have also made a lot of good research. Zhu et al. studied cascading failures in HK scale-free networks with tunable clustering coefficients under targeted attacks and found that the links around the removed nodes played two opposite roles in the load redistribution process. The redistributed load can be distributed more evenly to the neighbors of the removed node through these links, and they can also bring the catastrophic additional load to collapse more nodes. Simulations and analysis show that between the two effects moderate clustering networks that make the best compromise are the most robust [15]. Xu et al. have introduced a CML model based on cascading faults, where the perturbations are not uniformly distributed. The results show that to avoid cascades in the coupled map lattice, the network structure should be as uniform as possible [16]. Wang et al. proposed a coupled map lattice-based cascading failure model in which a given number of critical nodes are simultaneously perturbed. The results show that increasing the reconnection probability can reduce the scope of cascading faults, but increase the propagation speed of cascading faults. In addition, a more compact network structure will lead to a faster cascade fault propagation speed, and the propagation speed of the cascade is inversely proportional to the characteristic path length of the WS small-world network [17]. Ma et al. proposed a cascading failure model for k-uniform supernetworks based on CML theory. Simulation results show that hyper networks are more robust than general complex networks [18]. Du et al. used CML to model a complex public transportation network with multiple links and analyzed cascading failures under different external disturbances and coupling strengths [19]. Zhang et al. proposed an integrated coupled map lattice to assess the vulnerability of weighted urban rail transit networks and proposed a new passenger flow redistribution rule to discuss cascading failures of URTNs [20]. Sun et al. analyzed the statistical topology parameters of the Beijing rail transit network (BRTN) based on complex network theory. Then, a weighted BRTN cascading failure analysis model considering multiple static passenger flow loading and redistribution based on coupled map lattice is proposed [21].

In the research of UAV networks, there are research-related data on its vulnerability, mainly focusing on its network performance. Carlos et al. propose an identity and location validation scheme that combines a public-key-based authentication mechanism with a movement plausibility check for groups of UAVs. The key idea is to supplement the authentication mechanism by periodically checking the plausibility of the locations of neighboring UAVs, allowing the detection of intruders that are unable to follow expected trajectories [22]. Liu et al. investigate the performance of a downlink UAV integrated terrestrial cellular network (UTCN) and analytically study the influence of varying UAP altitude and density on the spatial throughput (ST) of UTCN [23]. Anjum et al. have derived the critical node density of coverage of the UNs using the

percolation theory, and adopted the comprehensive mobility model for UNs comprising of three key parameters such as speed, angular velocity, and pitch angle. By analyzing the theoretical analysis and simulation results, it has been affirmed that the proposed model can be used to estimate the critical node density to ensure the desired network coverage of UNs [24]. Cao et al. select six key indicators in the UAV Ad hoc network, including delay, delivery rate, throughput, link security, link stability, and mobility factor and use the classical ADC effectiveness evaluation model to quantitatively analyze and evaluate the task effectiveness of the UAV ad hoc network. That is an effective method to evaluate the effectiveness of the UAV Ad hoc network in a complex task environment [25].

3. Network Characteristics

In order to facilitate analysis, the general UAV network model can be abstracted by the nodes and edges of an undirected graph $G = (V, E)$, where $V = \{V_i | i = 1, 2, \dots, n\}$ represents the set of nodes, $E = \{(V_i, V_j) | i, j = 1, 2, \dots, n\}$ represents the set of edges, E_{ij} is the edge between node i and node j , and $n = |V|$ is the number of nodes in the graph G .

The network topology characteristics, such as the degree, the betweenness, and the clustering coefficient, are used to evaluate the state of each node in the network under the cascading failure.

3.1. Degree. The degree describes the direct influence of a node according to the number of its neighbor nodes. The degree of a node represents the number of edges connected to other nodes. In the UAV network, the degree could be degraded as the association of a UAV node to other UAV nodes in the UAV network. The degree is bigger, the quantity of UAV nodes to a selected UAV node is more. The degree of node i is written as

$$k_i = \sum_{j=1}^n a_{ij}, \quad (1)$$

where $A = (a_{ij})$ represents the adjacency matrix of the network, and $a_{ij} (a_{ij} \in (0, 1))$ represents the connection relationship between node i and node j . When $a_{ij} = 1$, node i is directly connected to node j . When $a_{ij} = 0$, node i is undirectly connected to node j .

3.2. Betweenness. The betweenness describes the load capacity of a node according to the amount of the shortest paths passing this node in a network, and it represents the force and influence of nodes or edges in the entire network. The betweenness of a node counts the fraction of the shortest paths passing through a given node, and it is an important evaluation index based on the paths in the network. In the UAV network, the distribution of betweenness represents the role of UAV nodes in the interaction of information

flow. The betweenness of node i is

$$B_i = \sum_{m=n} \frac{g_{mn}(i)}{g_{mn}}, \quad (2)$$

where $g_{mn}(i)$ represents the number of the shortest paths from node m to node n passing through node i , and g_{mn} represents the number of the shortest paths from node m to node n .

The betweenness of edge E_{ij} is

$$B_{ij} = \sum_{m=n} \frac{g_{mn}(E_{ij})}{g_{mn}}, \quad (3)$$

where $g_{mn}(E_{ij})$ represents the number of the shortest paths from node m to node n passing through edge E_{ij} .

3.3. Clustering Coefficient. The clustering coefficient describes the tightness among a node's neighbors according to the proportion of the number of edges connected to its neighbor nodes to the maximum number of the possible edges connected to its neighbors. The target of the clustering coefficient is to compare the degree of cohesion, and the clustering coefficient of a node reflects the possibility that its neighboring nodes are also connected. In the UAV network, the clustering coefficient can reflect the aggregation among UAV nodes. If the clustering coefficient is relatively large, it can be seen that there are many UAVs gathered here, and most of them are UAV groups flying in formation. Otherwise, the distribution of UAVs is scattered, and most of the UAVs fly in the network. The clustering coefficient of node i is

$$C_i = \frac{2s_i}{k_i(k_i - 1)}, \quad (4)$$

where s_i represents the number of triangles shaped by node i with its neighbors.

4. Vulnerability Evaluation of UAV Networks with Interference

4.1. The Interference Scenario. The UAV network may interfere with different features in practical applications, thus three different interference scenarios are set in this paper.

In the first interference scenario, we mainly focus on the situation where some important nodes in the UAV communication network are precisely interfered with by the outside world [26]. When the UAV network is in this interference scenario, the communication of some important nodes in the network, such as the control center, will be precisely affected, and the vulnerability of the network will be significantly increased in this case.

Some UAVs that play a key role in the UAV network are affected by electromagnetic interference and cannot work normally. That can affect the normal operation of many functions in the network. For example, in the UAV network, UAV nodes with a relatively large clustering coefficient are

usually the leaders of the UAV formation. When these nodes have interfered, other UAVs in the formation have no leadership, which will have a huge impact on the entire formation and even the entire network.

In the second interference scenario, this paper mainly focuses on the situation where the communication link in a certain frequency band in the UAV network is interfered with by the other party's signal [26]. In this paper, a part of the important communication links in the UAV network is disrupted by electromagnetic interference.

For example, after most of the links used for information exchange and data transmission in the drone network have interfered, the interaction between drones will become very difficult, which greatly affects the performance of the UAV network.

In the third interference scenario, the influence of the strength of the external interference on the UAV network [27] will be simulated in the paper. According to the intensity of the interference signal, the signals are divided into the suppressive interference signal, the strong interference signal, and the weak interference signal. The intensity of the suppressive interference signal considerably exceeds the intensity of the target signal, and the signal will make the target unable to communicate at the disturbing frequency. The strong interference signal uses large interference power in which the intensity equals the target signal's intensity or exceeds the target signal's intensity, and the signal makes it difficult to communicate at the disturbing frequency. The weak interference signal uses small interference power to disturb the enemy's communication. The interference intensity is less than the target signal's intensity, and it will make it more difficult to receive, but its communication form is not completely suppressed.

The importance of network nodes and links is measured according to indicators such as the degree and betweenness of network nodes and the connectivity of network links. If the interference is a selective attack based on the importance of nodes or links, it will have a serious impact on the connectivity of the network topology and greatly increase the vulnerability of the network.

4.2. Coupled Map Lattices Model. In the network, if the load on a node exceeds its computing capacity or the load on an edge exceeds its communication capacity, the node or the edge will fail, and its original load will be distributed to other edges or nodes according to a certain mechanism. However, once a complex network is formed, the topology of the network is fixed, and the capacity of each edge or node in the network is also fixed. As the load is redistributed, the load on other nodes and edges may exceed their original capacity, resulting in a new failed edge or node, and a new round of load redistribution, which may cause a chain reaction, or even cause the entire network crashes. This process is called the cascading failure of the network.

In network topology, each node has an initial state when it is running normally. When a network node is attacked deliberately, not only the current node will be removed but also the status of its neighbor nodes will be affected due to the adjacency between adjacent nodes. Based on the above

cascading failures theories, a coupled map lattice model is built to evaluate the vulnerability of the network from the perspective of topology.

The coupled map lattice is a dynamic system with discrete time, discrete space, and continuous state variables. Coupled map lattices have been extensively studied in simulating the dynamic behavior and cascading failures of complex networked systems. The model overcomes some of the shortcomings of traditional partial differential equations while ensuring high numerical calculation efficiency. In a network system modeled with a coupled map lattice, the cascading failure process can be well studied by observing the interactions between nodes and the changes in node states. A coupled map lattice model is built to describe the nonlinear system by the following procedure.

- (i) Select one or some state field variables on a grid
- (ii) Divide the system development process into a series of independent processes
- (iii) Each independent process is replaced by a simple parallel kinetic process on the grid, that is to say, the parallel nonlinear map of each grid point variable and the states of some neighbor points will be coupled with each other, or the above two processes develop independently in parallel
- (iv) Let each independent process proceed to complete the evolution of a time unit

According to the coupled map lattices theory, a reaction-diffusion process $\partial_t u$, which can be divided into a local reaction process $F(u)$ and a diffusion process $\varepsilon \nabla^2 u$, represented by

$$\partial_t u = F(u) + \varepsilon \nabla^2 u, \quad (5)$$

where u is the state vector, ε is the diffusion coefficient and i is the lattice coordinate.

The local reaction process can be described by parallel nonlinear mapping

$$x_i \longrightarrow x_i' = f(x_i), \quad (6)$$

where x_i is the state of this lattice i and the function f is a nonlinear mapping.

The diffusion process can be expressed by discretizing the Laplace operator, i.e., it corresponds to a second order difference equation

$$x_i' \longrightarrow x_i' + \frac{\varepsilon}{2} (x_{i+1}' + x_{i-1}') - \varepsilon x_i'. \quad (7)$$

According to Formula (8) and Formula (9), we can get a coupled map lattice model

$$x_i(t+1) = (1 - \varepsilon)f(x_i) + \frac{\varepsilon}{2} [f(x_{i+1}(t)) + f(x_{i-1}(t))], \quad (8)$$

According to the above formulas, considering the

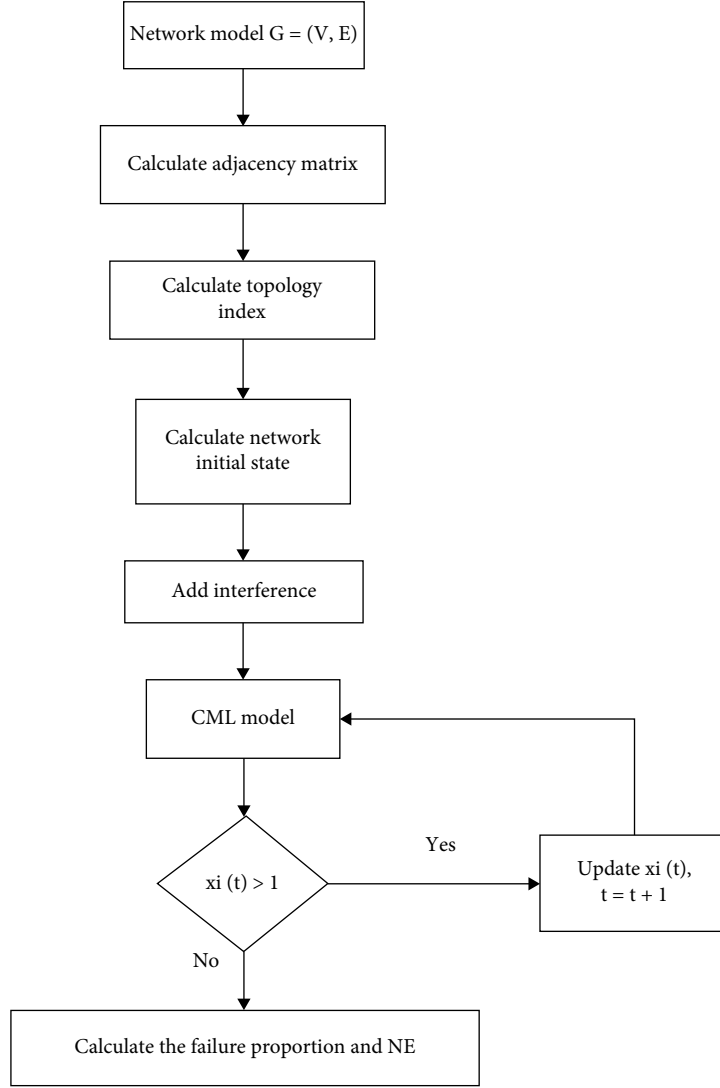


FIGURE 1: The process of the CML based on the cascading failure.

influence of adjacent nodes on the current node, the network topology features such as node degree, node betweenness, and clustering coefficient are integrated to construct a coupled graph model.

$$\begin{aligned}
 x_i(t+1) = & \left| (1 - \varepsilon_1 - \varepsilon_2 - \varepsilon_3)f(x_i(t)) + \frac{\varepsilon_1}{k_i} \sum_{j=1, j \neq i}^n a_{ij}f(x_j(t)) \right. \\
 & + \frac{\varepsilon_2}{\sum_{j=1, j \neq i}^n a_{ij}B_j} \sum_{j=1, j \neq i}^n a_{ij}B_jf(x_j(t)) \\
 & \left. + \frac{\varepsilon_3}{\sum_{j=1, j \neq i}^n a_{ij}C_j} \sum_{j=1, j \neq i}^n a_{ij}C_jf(x_j(t)) \right|, \quad (9)
 \end{aligned}$$

where $x_i(t)$ is the state of node i at time t , k_i is the degree of node i , a_{ij} represents the adjacency between node i and node j , B_i is the betweenness of node i , C_i is the clustering coefficient

of node i , $\varepsilon_i (i = 1, 2, 3)$ are the coupled coefficients of node degree, node betweenness and clustering coefficient, and $(\varepsilon_1 + \varepsilon_2 + \varepsilon_3) \leq 1$, $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in (0, 1)$.

The function f demonstrates the local dynamic behaviors which are chosen in this paper as the chaotic logistic map and establishes the relation between the nodes states at time t and the nodes states at time $t + 1$, $f(x) = 4x(1 - x)$, to demonstrate the evolution law of the network topology. If the initial state of all nodes in the interval $(0, 1)$ and there is no external perturbation, all the nodes will keep normal states. On the contrary, if node i exceeds its capacity constraint at the l -th time, the node i will be removed at this moment, and the state of the failed node will be assumed $x(i) \equiv 0$ at every later time.

This model integrates node degree, node betweenness, and clustering coefficient to describe the node state from their three perspectives. The integration is more suitable and comprehensive than the single aspect. In addition, the external perturbation R is involved in the expression of the

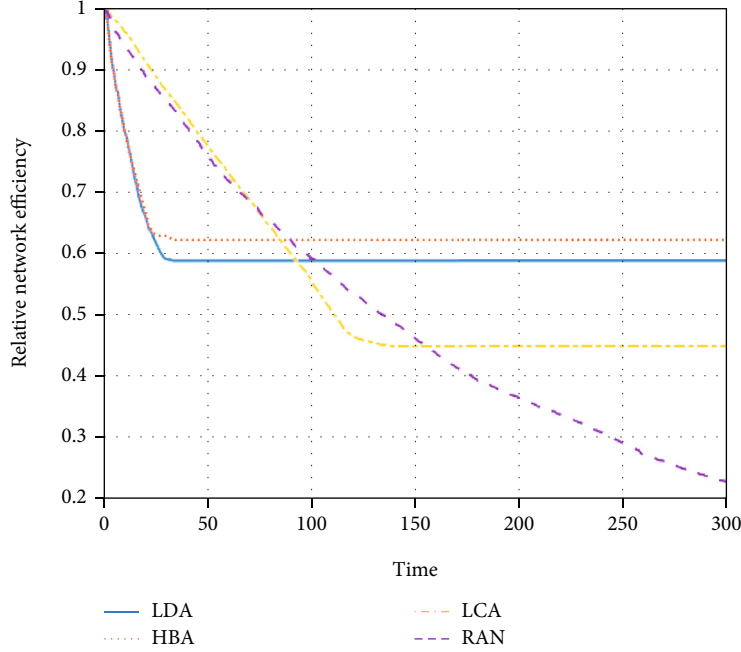


FIGURE 2: The evolution curve of relative NE under weak interference.

node state to imitate the failure intensity, therefore the node state under the external perturbation R can be represented by this formula.

$$\begin{aligned}
 x_i(t+1) = & \left| (1 - \varepsilon_1 - \varepsilon_2 - \varepsilon_3)f(x_i(t)) \right. \\
 & + \frac{\varepsilon_2}{\sum_{j=1, j \neq i}^n a_{ij} B_j} \sum_{j=1, j \neq i}^n a_{ij} B_j f(x_j(t)) \\
 & \left. + \frac{\varepsilon_3}{\sum_{j=1, j \neq i}^n a_{ij} C_j} \sum_{j=1, j \neq i}^n a_{ij} C_j f(x_j(t)) \right| + R.
 \end{aligned} \quad (10)$$

If node i fails at time t , then $x(i) = 0$, and the states of its neighbor nodes will be affected, so that the network transportation status will be recalculated at time $t + 1$. If the state of its neighbor node is larger than 1, the neighbor node will also fail and be removed from the network. If the condition is serious, the network will be broken.

Meanwhile, referring to the three interference scenarios mentioned in the first section above, the external disturbance R is defined and assigned in different ways.

In the first interference scenario, since the UAV network is faced with precise interference on important channels in this scenario, external interference R is added to the network in the form of interfering nodes. The interference strategies for nodes can be specifically divided into node degree interfering, node betweenness interfering, and clustering coefficient interfering, in addition, the random interference strategy is introduced as a comparison.

In the second interference scenario, since the UAV network faces a situation where some important communication links have interfered, external interference R is added

to the network in the form of a fraction of the edges with the largest betweenness of the concentrated interference edges.

In the third interference scenario, external interference R is divided into three types according to the intensity of the interference, suppressive interference, strong interference, and weak interference, respectively, to explore the specific influence of the external interference intensity on the network vulnerability.

4.3. Vulnerability Assessment Index. To analyze the network vulnerability, the nodes are selected according to several interference strategies while selecting the important UAV nodes to interfere with. In this paper, the relative network efficiency and the cascading failure proportion are used to evaluate the vulnerability of the network to disturbances.

The network efficiency (NE) is widely used to analyze the vulnerability in complex networks. NE is the average sum of the reciprocal of all shortest paths on the network and reflects the global connectivity of the network.

$$NE = \frac{1}{n(n-1)} \sum_{i=j} \frac{1}{L_{ij}}, \quad (11)$$

where L_{ij} is the shortest path length between node i and node j .

The relative network efficiency to assess the vulnerability of the network is presented as

$$NE = \frac{NE(\text{current})}{NE(\text{initial})}. \quad (12)$$

Meanwhile, the cascading failure proportion of the

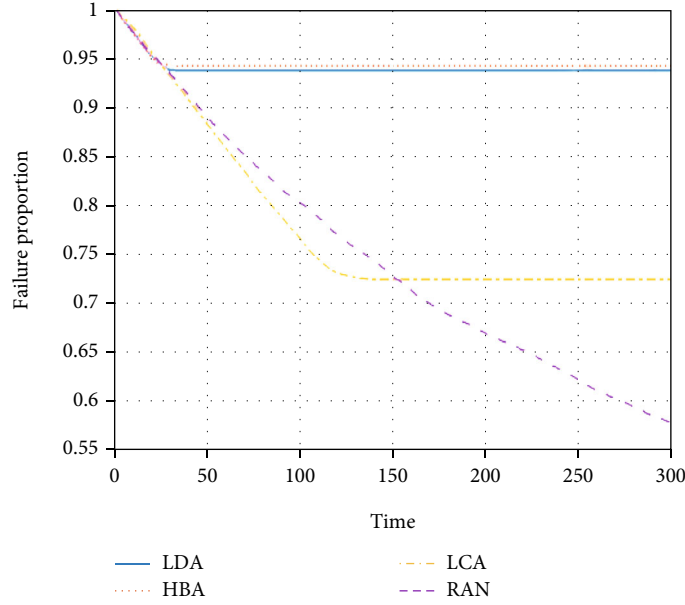


FIGURE 3: The evolution curve of failure proportion under weak interference.

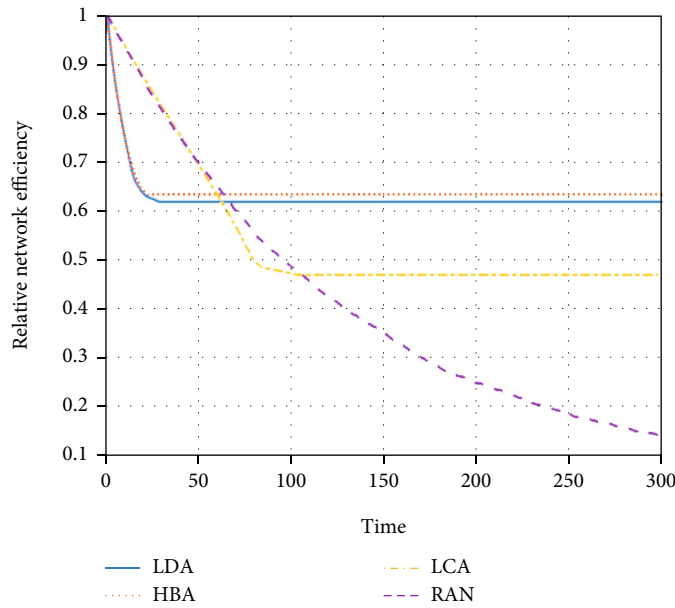


FIGURE 4: The evolution curve of relative NE under strong interference.

whole network is defined to assess the vulnerability of the network. The cascading failure proportion is the proportion of failed nodes from the initial state to the state after the cascading failure, which reflects the extent of the cascading failure caused by deliberate attacks on the network.

$$I_t = \frac{n_t}{n}. \quad (13)$$

where n_t is the number of remaining nodes in the network after the cascading failure.

4.4. Vulnerability Assessment Process. This paper constructs an assessment process for network vulnerability based on coupled map lattice model.

Firstly, generates a connectivity matrix of undirected graphs $A = (a_{ij})_{N \times N}$. Secondly, calculate the degree, the betweenness, and the clustering coefficients of all nodes in the network. Meanwhile, calculate the initial state of each node in the network and make the state of all the N nodes in the network normally. Then combine with the calculated results of the node importance index and use a different type of interference to select nodes with high importance and add interference at time t . For the nodes where the cascading

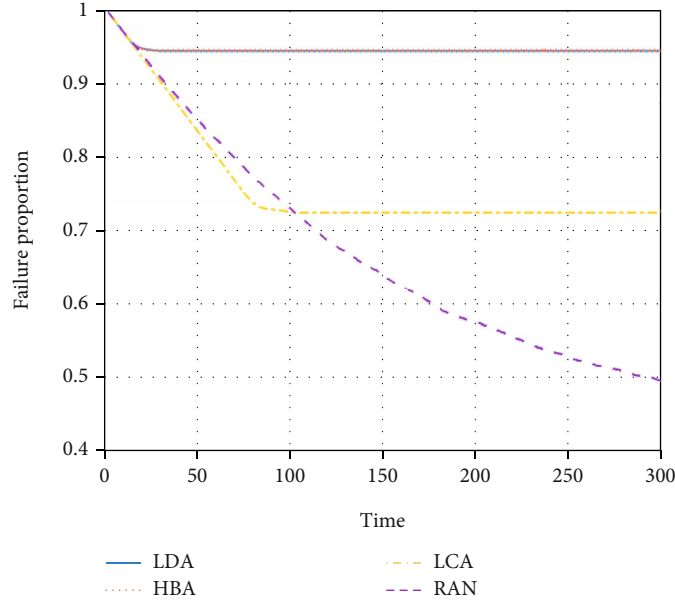


FIGURE 5: The evolution curve of failure proportion under strong interference.

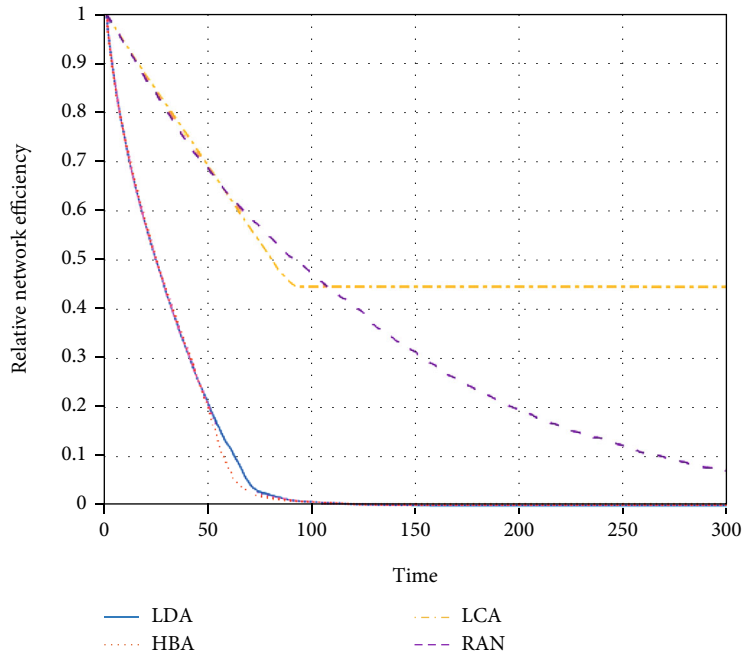


FIGURE 6: The evolution curve of relative NE under suppressive interference.

failure occurs, the coupled map lattices model is applied to update the state after time t for each node i in the network. During the iteration, other nodes do not add the interference except for the initially selected nodes. After a period of time, if there are no new failure nodes appearing in the network, the cascading failure phenomenon disappears naturally. Calculate the failure node ratio and relative network efficiency in the network to determine the influence range of the cascading failure and the vulnerability of the network.

In Figure 1, we plot a flow chart to demonstrate the process of the coupled map lattices based on the cascading failure model better in the interference scenario.

5. Simulation Result

This section assesses the network vulnerability from the perspective of multiple and uses the external disturbance R to simulate interference and to set R according to the

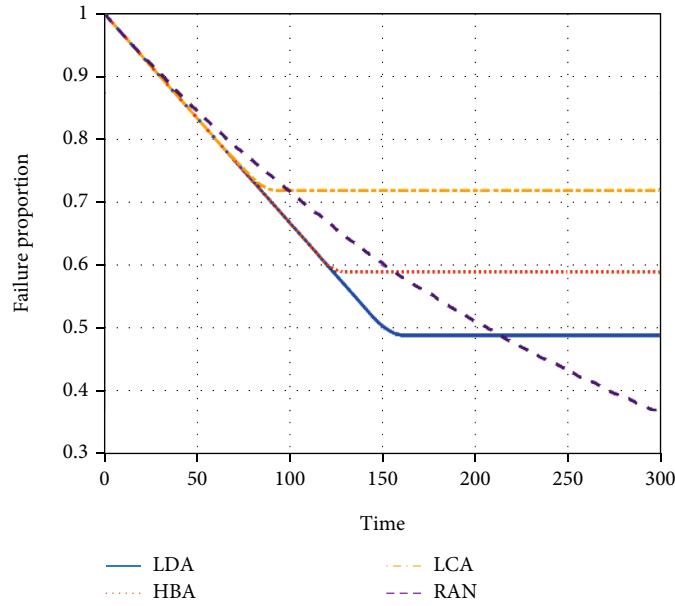


FIGURE 7: The evolution curve of failure proportion under suppressive interference.

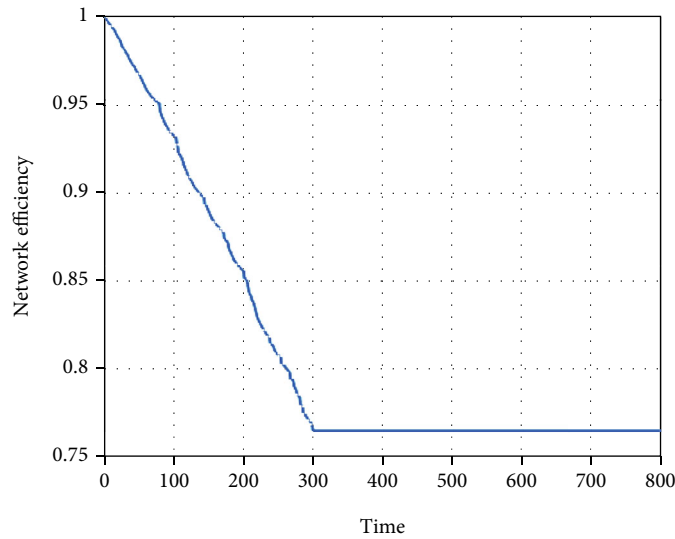


FIGURE 8: The evolution curve of NE in the second scenario.

interference of three different scenarios. We set three different types of interference strategies including the large degree interfering(LDA), the high betweenness interfering(HBA) and the large clustering coefficient interfering(LCA). At the same time, the proposed coupled map lattices model is used to evaluate the state of the nodes when the cascading failure occurs, and two evaluation parameters, failure proportion, and relative network efficiency are used to evaluate the vulnerability of the network. Referring to the scale-free and self-organizing characteristics of the UAV network, we take the scale-free network as the simulated network, which contains 300 nodes and the average node degree is 5.

5.1. Vulnerability Evaluation in First Scenario. In the first interference scenario, as shown in Figures 2 and 3, the weak

interference $R = 0.5$ is chosen as external interference. Taking the relative network efficiency as the evaluation parameter, for the nodes under the strategies based on LDA and HBA, the relative network efficiency will decline at a very fast speed at the beginning, but when it only drops to 63%, the relative network efficiency will flatten out and gradually stabilize. However, for the nodes under the strategy based on LCA, although the relative network efficiency initially declines slowly, it will eventually drop to about 47%. Compared with the three followings, random interfering shows the slowest decline trend, but it ultimately destroys more than the above three. At the same time, when the failure ratio is selected as the evaluation parameter, only 5% of nodes failed under the strategies based on LDA and HBA, failure nodes caused by LCA are more than 25%, while

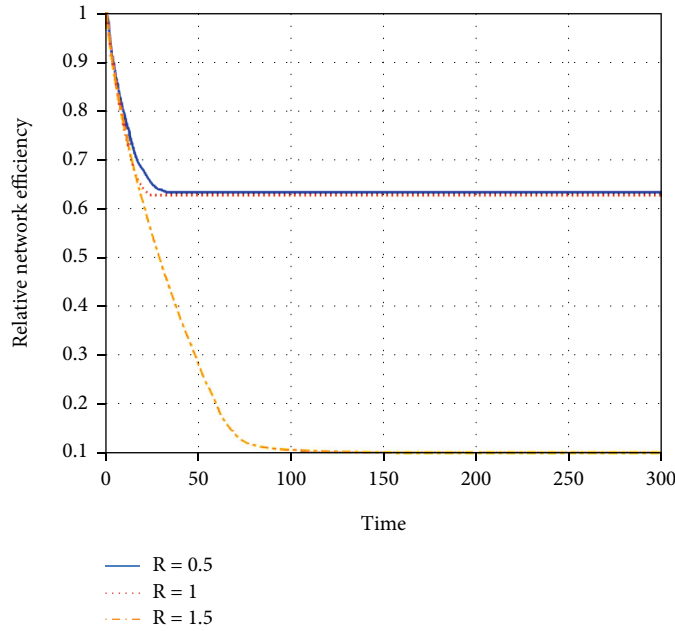


FIGURE 9: The evolution curve of relative NE under the LDA.

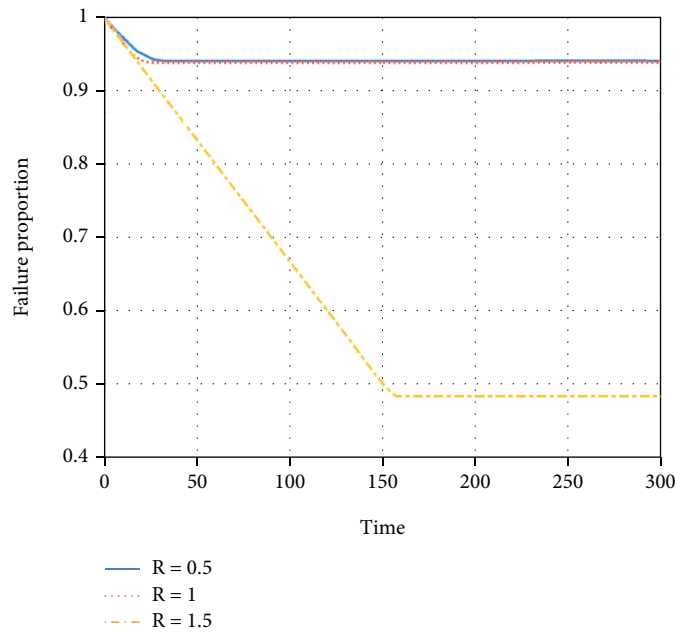


FIGURE 10: The evolution curve of failure proportion under the LDA.

61% of nodes under random interfering failed. The network will be more vulnerable under LCA. However, comparing the random interfering strategy, it can be seen that the failure rate is significantly faster under LDA and HBA.

As shown in Figures 4 and 5, the strong interference $R = 1$ is applied as the external disturbance. Under strong interference, the vulnerability of the network in these three strategies is almost not different from that under weak interference. Under the strategies based on LDA and HBA, the relative network efficiency drops to about 0.6, and it results that the failure proportion of the whole network dropping

about 5%, while under the strategy based on LCA, the network damages the most. The relative network efficiency drops to 44%, with more than 28% failed nodes. In other words, the network is more vulnerable under the strategy based on LCA, but under the random interfering strategy the vulnerability is the most obvious.

Next, as shown in Figures 6 and 7, the suppressive interference $R = 1.5$ is added as the external disturbance. Under the attack strategies based on LDA and HBA, the relative network efficiency almost drops to 0, but under the attack strategy based on LCA, it drops to about 44%. There are

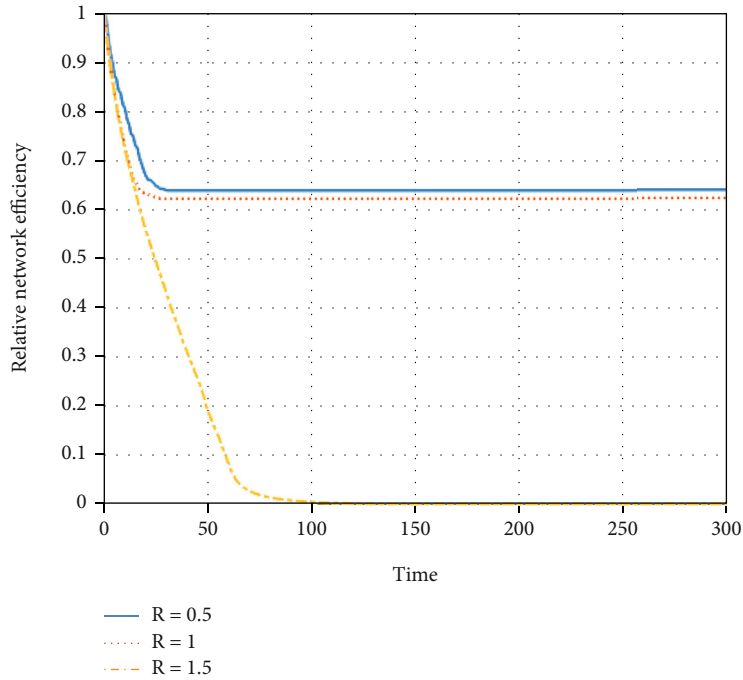


FIGURE 11: The evolution curve of relative NE under the HBA.

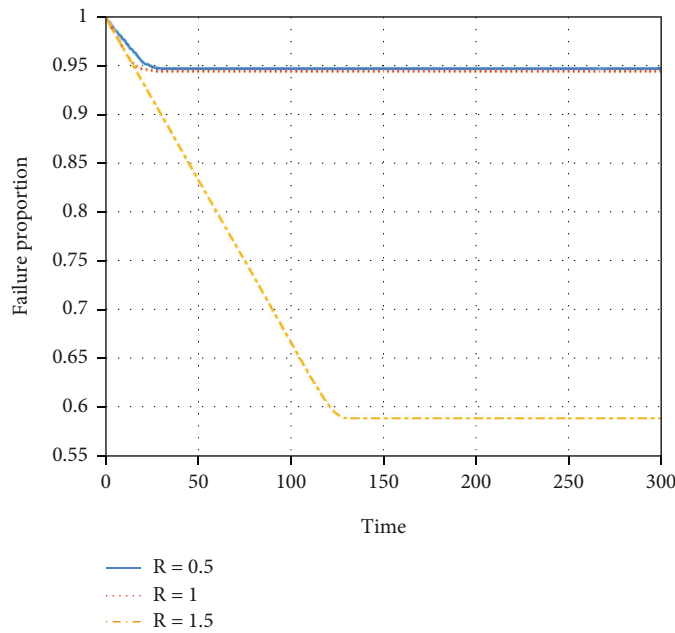


FIGURE 12: The evolution curve of failure proportion under the HBA.

52% nodes that failed under the LDA, 40% nodes failed under the HBA and 28% nodes failed under the LCA. Therefore, under inhibitory interference, the network almost collapses and collapses extremely fast under LDA and HBA, and the network is more vulnerable.

5.2. *Vulnerability Evaluation in Second Scenario.* In the second interference scenario, the relative network efficiency is taken as the evaluation parameter to perform large-scale

interference to multiple edges in the network according to the order of edge betweenness. Here, 800 edges with high edge betweenness are subjected to range interference. As it can be seen from Figure 8, the change in relative network efficiency only drops from 1 to about 0.76. Compared with the results obtained in the first interference scenario, it is obvious that in the case of network vulnerability, the precise attack based on the nodes is better than interfering within a range.

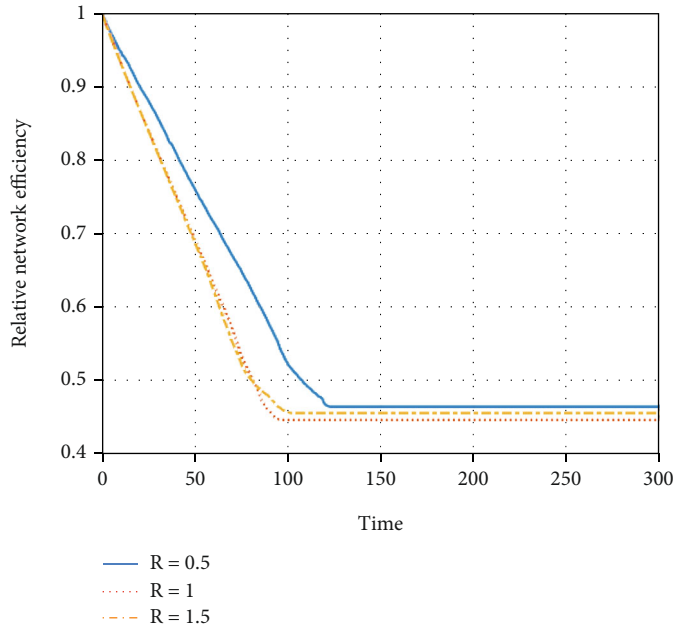


FIGURE 13: The evolution curve of relative NE under the LCA.

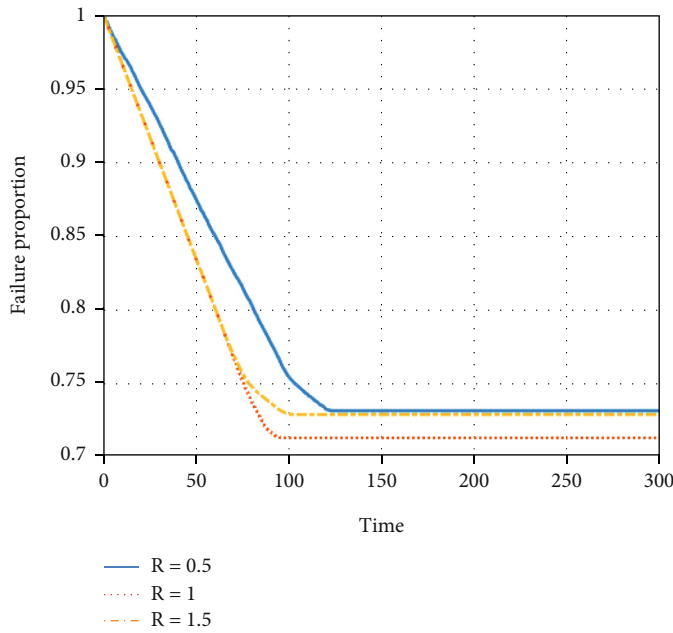


FIGURE 14: The evolution curve of failure proportion under the LCA.

5.3. *Vulnerability Evaluation in Third Scenario.* In the third interference scenario, we focus on the study of the impact of the same interference strategies on the network under different interference intensities. The relative network efficiency is also taken and the failure proportion of the whole network as evaluation indicators.

First of all, under the large node degrees interfering, we can see in Figures 9 and 10 that when the weak interference and the strong interference intensity, the network damage degree is small, compared to the initial state of the network, the relative network efficiency falls by about 38%, the failure

proportion of nodes is about 5.4%. But clearly, the increase in the intensity of interference makes the relative network efficiency and the failure ratio of nodes fall even faster. Secondly, when the external interference intensity is in the suppressive interference, the network destruction degree is greatly improved, the relative network efficiency drops to 0 and the failure proportion of nodes exceeds 50%, which almost leads to the collapse of the entire network. But compared with the strong interference intensity, the network efficiency and failure proportion decrease almost at the same speed. In addition, it can be seen from the figure that the

threshold of interference is about $R = 1$. Once the interference value exceeds the threshold, the vulnerability of the network will increase sharply.

Next, when node betweenness based interference strategies are studied, from Figures 11 and 12 that when the interference intensity is in the state of weak interference and strong interference, the relative efficiency of the network drops to about 36% and 39%, and the failure proportion of nodes is about 5%. The overall damage degree to the network is flat with the attack based on the large node degree. Meanwhile, it is obvious that as the intensity of interference increases, the network efficiency and failure ratio decrease faster. In addition, when the intensity of external interference is suppressive, the network damage degree is greatly improved, the relative network efficiency drops to 0, and the failure proportion of nodes is more than 41%, it almost causes the collapse of most of the network. Similarly, it can be seen from the figure that the threshold of interference is about $R = 1$. Once the interference value exceeds the threshold, the vulnerability of the network will increase sharply.

In addition, under the interference strategies based on clustering coefficients, from the simulation results in Figures 13 and 14 that no matter whether the interference intensity is in the weak interference state, strong interference state, or suppressed interference state, the final network damage degree caused by LCA has almost no difference. Compared with the initial state, the relative network efficiency decreases to 45% lower, and the failure proportion of the whole network is about 28%. The only difference is that as the intensity of the interference increases, the speed of the cascading failure increases. That is to say, the attack based on clustering coefficients is not obviously affected by the intensity of interference, and in this attack mode, the network will suffer a certain degree of damage but not very serious.

6. Conclusions

To sum up, we introduce a cascading failure model based on coupled map lattices. Take the scale-free network as an example to simulate the interference scenarios that the UAV network may encounter in practice, and study the network vulnerability changes in these scenarios. Furthermore, we set up three different important node interfering strategies for the scenario where the important UAV nodes in the UAV network are precisely interfered with. The simulation results show that the whole network will become more and more vulnerable with the increase of external interference intensity. At the same time, regardless of the intensity of external interference, the network under the large clustering coefficient interfering will be affected to a certain extent. Under the interference strategies based on a large degree and high betweenness, the network failure rate is extremely fast. When the interference is suppressive, the network is very vulnerable, and when the interference is small, the network's vulnerability is not obvious. In addition, it can be seen from the experimental data that the network is more vulnerable when the UAV node is subjected to electromagnetic interference, compared to interfering with a part of the communication link.

Therefore, in the face of external interference of high intensity, the first thing we need to do is to protect the nodes to a large degree and high betweenness in the network. In addition, when the intensity of external interference is small, we also need to notice the nodes of large clustering coefficients in the network.

The current work is to analyze the vulnerability of the UAV network considering the topology of the UAV network. The next work will start from the information interaction required by the network to complete its various functions according to the functions of the network, and further, analyze the vulnerability of the UAV network.

Data Availability

The data used to support the findings of this study are included in the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was supported in part by the National Key Research and Development Program of China (2020YFB1807700), the National Science Foundation of China (61701371,62002288,61971327), the China Postdoctoral Science Foundation (2017 M613073), the National Science Foundation for Young Scientists of Shaanxi (2020JQ-311), the Fundamental Research Funds for the Central Universities (Grant No. XJS200111), the Shaanxi Key Project under Grant 2020ZDLGY05-03, and the Ningbo Major Project under Grant 2019B10081.

References

- [1] Y. Wang, *Research on Connectivity Reliability of Urban Transit Network Based on Theory of Complex Network[J]*, Beijing Jiaotong University, Beijing, 2008.
- [2] D. M. Scott, D. C. Novak, L. Aultman-Hall, and F. Guo, "Network robustness index: a new method for identifying critical links and evaluating the performance of transportation networks," *Journal of Transport Geography*, vol. 14, no. 3, pp. 215–227, 2006.
- [3] P. Angeloudis and D. Fisk, "Large subway systems as complex networks," *Physica A: Statistical Mechanics and its Applications*, vol. 367, pp. 553–558, 2006.
- [4] W. Jing, X. Xu, and Y. Pu, "Route redundancy-based approach to identify the critical stations in metro networks: a mean-excess probability measure," *Reliability Engineering & System Safety*, vol. 204, article 107204, 2020.
- [5] O. Cats, G. J. Koppenol, and M. Warnier, "Robustness assessment of link capacity reduction for complex networks: application for public transport systems," *Reliability Engineering & System Safety*, vol. 167, pp. 544–553, 2017.
- [6] Z. Q. Liu and R. Song, "Reliability analysis of Guangzhou rail transit with complex network theory[J]," *Journal of Transportation Systems Engineering and Information Technology*, vol. 10, no. 5, pp. 195–200, 2010.

- [7] J. Zhang, X. Xu, L. Hong, S. Wang, and Q. Fei, "Networked analysis of the Shanghai subway network, in China," *Physica A: Statistical Mechanics and its Applications*, vol. 390, no. 23-24, pp. 4562-4570, 2011.
- [8] L. Hong, X. Zhong, M. Ouyang, H. Tian, and X. He, "Vulnerability analysis of public transit systems from the perspective of urban residential communities," *Reliability Engineering & System Safety*, vol. 189, pp. 143-156, 2019.
- [9] J. Johansson and H. Hassel, "An approach for modelling interdependent infrastructures in the context of vulnerability analysis," *Reliability Engineering & System Safety*, vol. 95, no. 12, pp. 1335-1344, 2010.
- [10] J. Sienkiewicz and J. A. Hołyst, "Statistical analysis of 22 public transport networks in Poland," *Physical Review E*, vol. 72, no. 4, article 046127, 2005.
- [11] L. G. Mattsson and E. Jenelius, "Vulnerability and resilience of transport systems-a discussion of recent research[J]," *Transportation Research Part A: Policy and Practice*, vol. 81, pp. 16-34, 2015.
- [12] Y. Yang, Y. Liu, M. Zhou, F. Li, and C. Sun, "Robustness assessment of urban rail transit based on complex network theory: a case study of the Beijing Subway," *Safety Science*, vol. 79, pp. 149-162, 2015.
- [13] D. J. Sun and S. Guan, "Measuring vulnerability of urban metro network from line operation perspective[J]," *Transportation Research Part A: Policy and Practice*, vol. 94, pp. 348-359, 2016.
- [14] Q. Lilin, W. Muqing, and Z. Min, "Identification of key nodes in complex networks," in *2021 7th International Conference on Computer and Communications (ICCC)*, pp. 2230-2234, Chengdu, China, 2021.
- [15] X. J. Zhang, B. Gu, X. M. Guan, Y. B. Zhu, and R. L. Lv, "Cascading failure in scale-free networks with tunable clustering," *International Journal of Modern Physics C*, vol. 27, no. 8, p. 1650093, 2016.
- [16] K. J. Xu, C. Hong, X. H. Zhang, Q. H. Sun, N. He, and M. M. Xiao, "Cascades in coupled map lattices with heterogeneous distribution of perturbations," *Physica A: Statistical Mechanics and its Applications*, vol. 547, article 123839, 2020.
- [17] E. S. Wang, C. Hong, X. H. Zhang, and N. He, "Cascading failures with coupled map lattices on Watts-Strogatz networks," *Physica A: Statistical Mechanics and Its Applications*, vol. 525, pp. 1038-1045, 2019.
- [18] X. Ma, F. Ma, J. Yin, and H. Zhao, "Cascading failures of k uniform hyper-network based on the hyper adjacent matrix," *Physica A: Statistical Mechanics and Its Applications*, vol. 510, pp. 281-289, 2018.
- [19] W. Du, J. Yu, X. An, and C. Ma, "Cascading failures of complex public transit network with multi-links based on CML[J]," *Transportation Research*, vol. 1, no. 6, pp. 14-19, 2015.
- [20] J. Zhang, Z. Wang, S. Wang, W. Shao, X. Zhao, and W. Liu, "Vulnerability assessments of weighted urban rail transit networks with integrated coupled map lattices," *Reliability Engineering & System Safety*, vol. 214, article 107707, 2021.
- [21] L. Sun, Y. Huang, Y. Chen, and L. Yao, "Vulnerability assessment of urban rail transit based on multi-static weighted method in Beijing, China," *Transportation Research Part A: Policy and Practice*, vol. 108, pp. 12-24, 2018.
- [22] "UAVouch: a secure identity and location validation scheme for UAV-Networks," *Access*, vol. 9, pp. 82930-82946, 2021.
- [23] J. Liu, M. Sheng, R. Lyu, and J. Li, "Performance analysis and optimization of UAV integrated terrestrial cellular network," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1841-1855, 2019.
- [24] M. N. Anjum, H. Wang, and H. Fang, "Coverage analysis of random UAV networks using Percolation theory," in *2020 International conference on computing, Networking and Communications (ICNC)*, pp. 667-673, Big Island, HI, USA, 2020.
- [25] J. Cao, C. Liu, Z. Dong, and P. Wang, "Effectiveness evaluation of UAV Ad hoc network in complex task environment," in *2021 International Conference on Communications, Information System and Computer Engineering (CISCE)*, pp. 745-748, Beijing, China, 2021.
- [26] S. Jeong and C. S. Sin, "GNSS interference signal generation scenario for GNSS interference verification platform[C]," in *2015 15th international conference on control, automation and systems (ICCAS)*, pp. 1363-1365, Busan, Korea, 2015.
- [27] G. S. Wang, Q. H. Ren, and Y. Z. Su, "The interference classification and recognition based on SF-SVM algorithm[C]," in *2017 IEEE 9th international conference on communication software and networks (ICCSN)*, pp. 835-841, Guangzhou, China, 2017.