Robustness Study of Non-Uniform Scale-Free Hyper-Network Structure

Bin Zhou[1,2], Xiujuan Ma[1*], Fuxiang Ma[1]

[1]*School of Computer, Qinghai Normal University, Xining, China;*
[2]*The State Key Laboratory of Tibetan Intelligent Information Processing and Application, Xining, China*

Abstract

The relationship between the internal structure of the hyper-edge and robustness of the hyper-network has not yet been investigated. Aiming at this problem, this paper proposes a hyper-network capacity-load model with non-uniform load distribution. And obtained the robustness of the non-uniform scale-free hyper-network under different internal structures of the hyper-edge. The simulation reveals that the robustness of the non-uniform scale-free hyper-network is closely related to the internal structure of the hyper-edge. The non-uniform scale-free hyper-network is most robust when the nodes inside the hyper-edges are fully connected. The results show that the internal structure of hyper-edge has a large impact on the overall robustness of the non-uniform scale-free hyper-network.

Keywords

non-uniform scale-free hyper-network; the capacity-load model; hyper-network structure; robustness

1 Introduction

Nowadays, complex networks have become an effective tool for modeling all kinds of complex systems [1]. For many realistic complex systems, robustness is their most essential system performance. In recent years, researchers have also successfully investigated the robustness of various complex systems based on complex network theory [2-4]. However, with the development of the times, various systems in production life are becoming more and more complex. The graph-based theory of complex networks is no longer a good representation of complex system structures [5,6]. The emergence of hyper-network theory has brought new research methods to study such complex systems. Hyper-edges in a hyper-network can better represent some complex relationship between multiple nodes at the same time. Therefore, hyper-networks have been used to model many real complex systems [7-9]. Although the modeling research of hyper-network has become more and more mature, because of the complex structure of hyper-network, the research on the robustness of hyper-network is still in its infancy. Ma et al. [10] found through research that the hyper-network is more robust to the same external disturbance than the ordinary network. Chen et al. [11] found that random hyper-network and small-world hyper-network are more robust than random networks and smallworld networks. And the robustness of random hyper-network is stronger than small-world hyper-network. However, the above works do not consider the relationship between the internal structure of the hyper-edge and the robustness of the hyper-network. In real life, the influence of microstructure on macrostructure cannot be ignored. For example, in integrated circuit development [12], studying the connection relationship between electronic components inside the integrated functional block can further optimize the robustness of the integrated circuit. Therefore, studying the relationship between the internal structure of the hyper-edge and the robustness of the hyper-network can provide a more comprehensive knowledge and understanding of the factors influencing the robustness of the hyper-network, and thus can propose better optimization strategies to improve the resistance of the hyper-network to various types of attacks.

AIoTC2022@International Conference on Artificial Intelligence, Internet of Things and Cloud Computing Technology
EMAIL: *Corresponding author's email: qhnumaxiujuan@163.com (Xiujuan Ma)

In this paper, based on non-uniform scale-free hyper-networks [13], the internal structure of the hyper-edges is considered, three non-uniform scale-free hyper-networks with different structures inside the hyper-edges are constructed, and a capacity-load model applicable to the hyper-networks is proposed based on the idea of the capacity-load model [14], and the relationship between the internal structure of the hyper-edges and the robustness of the non-uniform scale-free hyper-networks is investigated.

2 Research Methodology

2.1 The concept of hyper-graph

The concept of hyper-graph, defined as follows. If the binary relation H=(V,E) satisfies the condition [15] :

1) $\emptyset = e_i \in P(V)$, $i \in \{1,2,\cdots,m\}$;

2) $\cup_{i=1}^{m} = V$.

where the elements in the set V are calledthe nodes or vertices of the hyper-graph, and the elements in E are called the hyper-edges of the hyper-graph. $P(V)$ denotes the power set of the set V; then H is a hyper-graph. The hyper-graph of a node i in a hyper-graph is defined as the number of hyper-edges containing the node i, denoted as $d_H(i)$ [16]. The node degree of node i is similar to that of a normal network and isstill defined as the number of normal edges associated with node i, denoted as $d(i)$ [16]. The ordinary degree of node i within a separate hyper-edge e_i is denoted as $k_{e_i}(i)$. The number of nodes contained within a hyper-edge is denoted as the order of this hyper-edge, denoted as $o(e_i)$.

2.2 Hyper-network capacity-load model

Inspired by the capacity-load model proposed by Motter [14], we propose a cascade model under the load local redistribution rule. In our model, the main differences from previous models are as follows.

(1) In a hyper-network with N nodes, the initial load of node i is related to the hyper-degree $d_H(i)$ and node degree $d(i)$ of that node, and its initial load $L_i(0)$ is defined as

$$L_i(0) = \alpha(d_H(i) + d(i))^{\beta}, \alpha \geq 1, \beta \geq 1 \tag{1}$$

In order to control the initial load of node i, let α be the load parameter and β be the adjustable parameter.

(2) The load on the failed node i will be distributed to node j in 2 steps.

Step 1: First assign to its associated unfailed hyper-edges according to the priority probability.

$$\prod\nolimits_{hyper-edge} = \frac{o(e_i)}{\sum\limits_{m \in E_i} o(e_m)} \tag{2}$$

where E_i denotes the set of all associated hyper-edges of the faulty node i.

Step 2: After the faulty node i assigns the load to its adjacent unfailed hyper-edges according to the above equation, it continues to assign according to the priority probability Π_{node}.

$$\prod\nolimits_{node} = \frac{k_{e_i}(i)}{\sum\limits_{r \in \Gamma_i} k_{e_i}(r)} \tag{3}$$

where Γ_i denotes the set of all unfailed neighbor nodes of the faulty node i within the hyper-edge e_i.

Then the load received by node j is shown in equation (4).

$$\Delta L_{ji} = L_i \times \Pi_{hyper-edge} \times \Pi_{node} \tag{4}$$

From equation (4), it can be seen that the additional load received by node j within the hyper-edge

e_i is related to the order of the hyper-edge it is on, the commonness of node j within the hyper-edge e_i, and the initial load of node i.

In a realistic hyper-network, the capacity is the maximum value of the load that a node or hyper-edge can handle, proportional to the initial load of the node. Let the capacity of node j be, expressed by equation (5).

$$C_j = (1+T)L_j \quad T \geq 0 \tag{5}$$

Here T is the capacity parameter, the larger the value of T, the higher the capacity of the node and the more resilient it is to failures, but the cost of resilience increases. The critical threshold T_C is the minimum capacity value to avoid global collapse of the hyper-network. When $T>T_C$, the entire hyper-network does not experience a global collapse. When $T<T_C$, the whole hyper-network will experience a global collapse. Therefore, the critical threshold T_C of T is an important indicator of the robustness of the hyper-network. Obviously, a smaller T_C indicates a more robust hyper-network.

If node j fails after obtaining additional load, it should satisfy the following inequality.

$$L_j + \Delta L_{ji} > C_j \tag{6}$$

If equation (6) holds, then node j will overload and fail, which may cause other nodes to fail when node j 's load is redistributed.

To measure the robustness of the hyper-network, node i is initially attacked and made to fail, and then its load is redistributed. For other nodes after load redistribution, the node fails if equation (6) is satisfied. When all nodes within a hyper-edge fail, then this hyper-edge fails. After the number of failed nodes in the hyper-network reaches a steady state or all nodes fail (global collapse), the number of failed hyper-edges F_M ($0 \leq F_M \leq$ M) in the hyper-network is counted and the percentage of hyper-edge failure f_M is calculated as shown in equation (7).

$$f_M = \frac{F_M}{M}, 0 \leq f_M \leq 1 \tag{7}$$

Where M is the total number of hyper-edges in the hyper-network. From equation (7), it can be seen that a larger f_M indicates a larger number of failed hyper-edges in the hyper-network, i.e., the less robustness of the hyper-network.

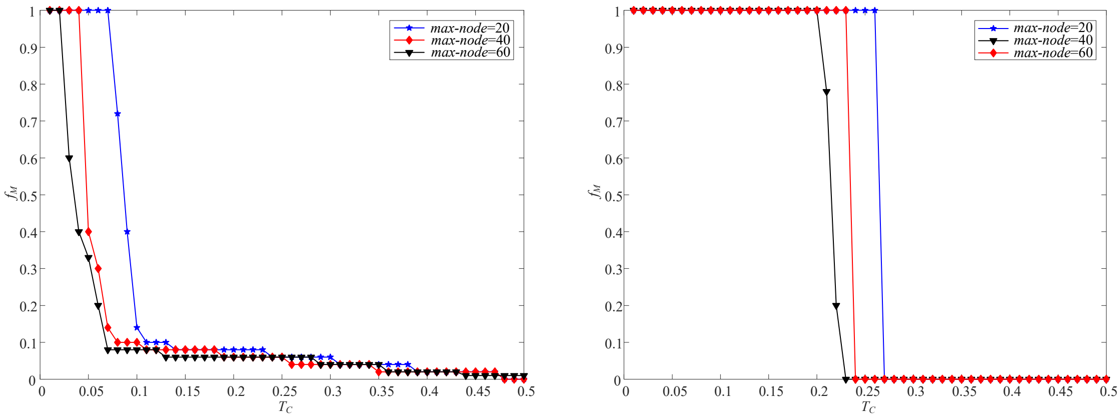
3 Simulation experiments

In analyzing the relationship between the internal structure of non-uniform scale-free hyper-network hyper-edge and the robustness of the hyper-network, this paper constructs three hyper-networks: the non-uniform scale-free hyper-network with preferentially connected nodes inside the hyperedge is denoted as NON-BA-P hypernetwork; the non-uniform scale-free hyper-network with stochastically connected nodes inside the hyperedge is denoted as NON-BA-S hypernet-work; the non-uniform scale-free hyper-network with fully connected nodes inside the hyperedge is denoted as NON-BA-F hypernetwork. And simulates the cascading failure process of the non-uniform scale-free hyper-network with different structures inside the three hyper-edges under two strategies of deliberate attack and random attack simulations, and the related experimental data are recorded. The random attack in the simulation experiment is to randomly select a node in the hyper-network to attack; while the deliberate attack is to select the node in the hyper-network that satisfies the maximum sum of node degree value and node hyperdegree to attack.

The size of each type of hyper-network is related to the parameter max-node, so in order to perform simulation analysis at different sizes, three sizes of networks with max-node of 20, 40 and 60 are used in this paper. The focus of this paper is to discover the influence of the internal structure of the hyper-edge on the robustness of the hyper-network, and to eliminate the influence of other uncertainties on the robustness, we use the control variable method, i.e., the parameter α is taken as 10 and the parameter β is taken as 1. To ensure the validity and authenticity of the results, the experimental results are taken as the average of 100 times results.

3.1 Robustness of the NON-BA-P hyper-network

Fig.1 represents the variation of the NON-BA-P hyper-network's hyper-edge failure ratio f_M with the capacity parameter T when it is under attack at different maximum number of nodes within the hyper-edge max-node. It is obvious from Figs.1(a) and (b) that the critical threshold T_C of the NON-BA-P hyper-network becomes gradually smaller as the max-node increases, and since the smaller the T_C, the more robust the hyper-network is, it can be concluded that the robustness of the NON-BA-P hyper-network increases with the increase of the hyper-network size. the NON-BA-P hyper-network is robust to random attacks and vulnerable to deliberate attacks.

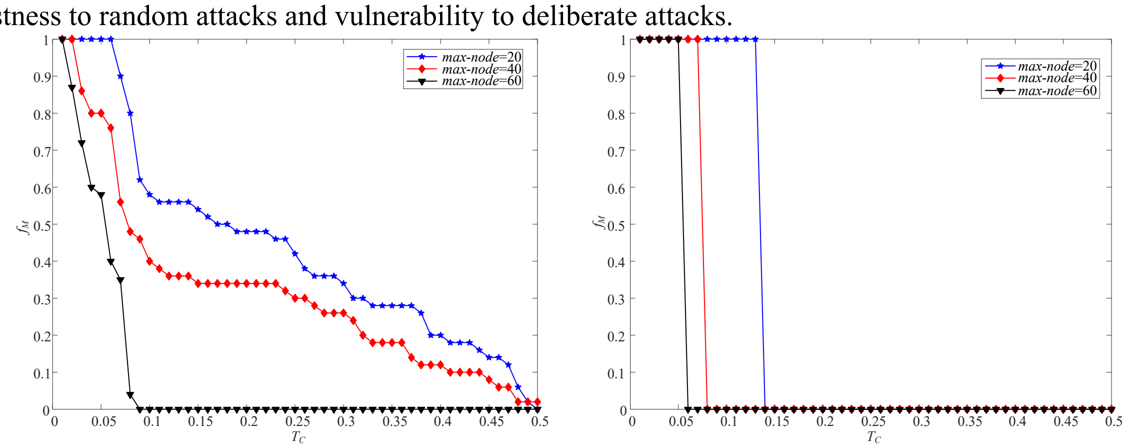


(a)random attacks (b)deliberate attacks

Figure 1 NON-BA-P hyper-network hyper-edge failure ratio under different capacity parameters

3.2 Robustness of the NON-BA-S hyper-network

Fig.2 represents the variation of the NON-BA-S hyper-network's hyper-edge failure ratio f_M with the capacity parameter T under different maximum number of nodes max-node within the hyper-edge when it is under attack. It is obvious from Figs.2(a) and (b) that the larger the max-node, the smaller the critical threshold T_C of the NON-BA-S hyper-network, and since the smaller the T_C, the more robust the hyper-network is, it can be concluded that the robustness of the NON-BA-S hyper-network likewise increases with the increase of the hyper-network size. the NON-BA-S hyper-network also exhibits robustness to random attacks and vulnerability to deliberate attacks.

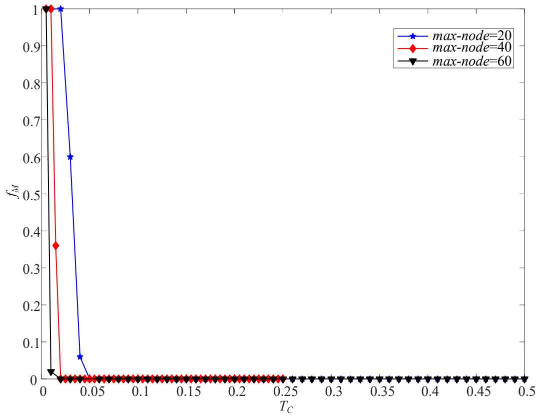


(a)random attacks (b)deliberate attacks

Figure 2 NON-BA-S hyper-network hyper-edge failure ratio under different capacity parameters

3.3 NON-BA-F Hyper-Network Robustness

Figs.3(a) and (b) further verify that the critical threshold T_C of the NON-BA-F hyper-network is smaller when the max-node is larger. And the robustness of the NON-BA-F hyper-network also increases with the increase of the size of the hyper-network. The NON-BA-F hyper-network again exhibits the property of being robust to random attacks and vulnerable to deliberate attacks.



(a)random attacks (b)deliberate attacks

Figure 3 NON-BA-F hyper-network hyper-edge failure ratio under different capacity parameters

3.4 Comparative analysis of three non-uniform scale-free hyper-networks

We found through simulation experiments that the three non-uniform scale-free hyper-networks show a decreasing trend of hyper-edge failure ratio with the increase of capacity parameter value under two strategies of deliberate attack and random attack, and reach the critical threshold of global collapse under a certain capacity parameter. When $T \le T_C$, all three non-uniform scale-free hyper-networks are in the state of global collapse, and when $T > T_C$, the failure scale starts to decrease and finally reaches the state of global non-failure. In order to observe the change of the critical threshold more conveniently and intuitively, we give the data tables of the three non-uniform scale-free hyper-networks when the maximum number of nodes within the hyper-edge is 20,40,60, respectively, as shown in Table 1.

Table 1 The critical threshold by three non-uniform scale-free hyper-networks under different size of nodes max-node

	random attacks			deliberate attacks		
max-node	20	40	60	20	40	60
NON-BA-P	0.07	0.04	0.02	0.26	0.23	0.2
NON-BA-S	0.06	0.02	0.01	0.13	0.07	0.05
NON-BA-F	0.02	0.01	0.005	0.04	0.02	0.01

We find that different structures inside the hyper-edge have different effects on the robustness of the hyper-network. When the internal structure of the hyper-edge is fully connected, the non-uniform scale-free hyper-network is the most robust; followed by when the internal structure of the hyper-edge is randomly connected, the non-uniform scale-free hyper-network robustness is at a medium level; when the internal structure of the hyper-edge is preferentially connected, the non-uniform scale-free hyper-network robustness is the worst.

4 Conclusion

In order to break through the limitations of the existing research on the structural robustness of hyper-networks and explore the relationship between the internal structure of hyper-edges and the robustness of hyper-networks, we propose three hyper-edges with different internal structure of non-uniform scale-free hyper-networks models, and propose a non-uniformly distributed capacity-load model of hyper-networks, and analyze the influence of the internal structure of hyper-edges on the overall robustness of non-uniform scale-free hyper-networks. The following conclusions are obtained: the internal structure of the hyper-edge has an important influence on the robustness of the non-uniform scale-free hyper-network, and the robustness of the non-uniform scale-free hyper-network is strongest when the internal structure of the hyper-edge is fully connected; the robustness of the non-uniform scale-free hyper-network is worst when the internal structure of the hyper-edge is preferentially connected. And when the maximum size number max-node of nodes inside the hyper-edge is larger, the robustness of the non-uniform scale-free hyper-network is stronger.

5 Acknowledgments

This work is supported by Natural Science Foundation of Qinghai Province in China (NO. 2019-ZJ-7012) and the National Natural Science Foundation of China (NOS. 11801296, 61603206).

6 References

[1] Santos F., Aquino A. L. L., Madeira E. R. M., et al: Temporal complex networks modeling applied to vehicular ad-hoc networks, Journal of Network and Computer Applications. Vol. 192, 2021, pp. 103168

[2] Wang Z., Li J. H., Kang D., et al: Review on strategies enhancing the robustness of complex network, Complex Systems and Complexity Science. Vol. 17, 2020, pp. 1-26+46

[3] Wang S. L., LYU W. Z., Zhang J. H., et al: Method of power network critical nodes identification and robustness enhancement based on a cooperative framework, Reliability Engineering & System Safety. Vol. 207, 2021, pp. 107313

[4] Gao J., Buldyrev S. V., Havlin S., et al: Robustness of a network formed by n interdependent networks with a one-to-one correspondence of dependent nodes, Physical Review E. Vol. 85, 2012, pp. 066134

[5] Federico B., Giulia C., Iacopo I., et al: Networks beyond pairwise interactions: Structure and dynamics, Physics Reports. Vol. 874, 2020, pp. 1-92

[6] Sinan G. A., Cliff J., Carlos O. M., et al: Hypernetwork science via high-order hypergraph walks, EPJ Data Science. Vol. 9, 2020, pp. 519-535

[7] Li M. N., Guo J. L., Bian W., et al: Tang poetry from the perspective of network, Complex Systems and Complexity Science. Vol. 14, 2017, pp. 66-71

[8] Hu F., Zhao H. X., Zhao J. B., et al: An evolving model for hypergraph-structure-based scientific collaboration networks, Acta Physica Sinica. Vol. 62, 2013, pp. 547-554

[9] Hu F., Liu M., Zhao J., et al: Analysis and application of the topological properties of protein complex hypernetworks, Complex Systems and Complexity Science. Vol. 15, 2018, pp. 31-38

[10] Ma X. J., Zhao H. X., Hu F.: Cascading failure analysis in hyper-network based on the hypergraph, Acta Physica Sinica. Vol. 65, 2016, pp. 374-383

[11] Chen Y., Ma X. J., Ma F. X., et al: The Capacity Load Model of K-Uniform Hyper-Network based on Equal Load Distribution, Journal of Physics: Conference Series. Vol. 1828, 2021, pp. 012060

[12] Jiang Y., Wu S., Yang H., et al: Secure Data Transmission and Trustworthiness Judgement Approaches Against Cyber-Physical Attacks in an Integrated Data-Driven Framework, IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2022.

[13] Chen Y.: Research on the cascading failures model and application of hypernetwork based on capacity-load. Qinghai Normal University, 2021.

[14] Motter A. E., Cheng L. Y.: Cascade-based attacks on complex networks, Physical Review E. Vol. 66, 2002, pp. 065102

[15] Berge C.: Graphs and Hpergraphs. New York: Elsevier, 1973.

[16] Bretto A.: Hypergraph Theory. Springer, Heidelberg, 2013.