Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

Disintegrate hypergraph networks by attacking hyperedge

Hao Peng [a], Cheng Qian [a], Dandan Zhao [a], Ming Zhong [a], Xianwen Ling [a], Wei Wang [b,*]

[a] College of Mathematics and Computer Science, Zhejiang Normal University, Jinhua 321004, China
[b] School of Public Health and Management, Chongqing Medical University, Chongqing 400016, China

ARTICLE INFO

Article history:
Received 30 January 2022
Revised 29 March 2022
Accepted 27 April 2022
Available online 10 May 2022

Keywords:
Hypergraph network
Target attack
Percolation theory
Cascading failures

ABSTRACT

Throughout the last two decades, complex systems have been modeled as complex networks by capturing pairwise interactions. However, as research has progressed, it has been shown that many systems would lose much useful information after modeling the pairwise interaction relationship. According to study results, higher-order interactions are becoming more generally accepted as an essential element of complex systems. Hypergraphs may be used to explore the relationships between higher-order structures and functions in complex systems and capture higher-order interactions. After the initial failure of a hypergraph network, cascading failures may occur, just as they can with a simple network. Previous research has concentrated on random initial failures, and how hypergraph networks adapt to targeted attacks remains unanswered. In this research, we build a mathematical framework to explore the robustness of hypergraph networks against targeted attacks based on the magnitude of the hyperedge's cardinality. We discovered that when the probability of large cardinality hyperedges being deleted grows, the network becomes more fragile.

1. Introduction

In the past twenty years, the theory of network science has been developing and improving (Newman et al., 2010; Cohen et al., 2010). In recent years, researchers have found that many systems modeled by pairwise interaction will lose some important information in the network. Because more and more research results show that higher-order interaction is considered as a basic aspect of complex systems, such as brain neural network and social contact network (Zhao et al., 2022; G. Ghoshal et al., 2009; Li et al., 2022).

The network describes the universal connection between different things in the objective world. Usually, this kind of connection is expressed through a pairwise interaction relationship; that is, if there is some connection between two objective objects, according to the theory of network science (Shao et al., 2009; Newman, 2002), there is an edge between the nodes corresponding to the objects when constructing the network (Bondy et al., 1976; Berahmand et al., 2021; Peng et al., 2020). However, in the real world, there are higher-order relationships. Like social networks (Singh et al., 2021), there are interactive relationships between different social media users, such as exchanging messages and paying attention to each other in the same group. In this case, a simple network can not accurately describe the relationship between users but needs to design a hypergraph network to describe the dynamic operation and interaction between social users. For example, a hyperedge can represent a group of closely interacting users who are regarded as nodes in a hypergraph network (Alotaibi and Rhouma, 2021; Wang et al., 2018; Zhou et al., 2020).

A simple graph consists of nodes and edges. If there is a relationship between two nodes, edges connect them. The node's degree is the number of edges connecting to a node in an undirected graph. Hypergraph (Bretto, 2013) is the extension of the graph; the number of nodes contained by hyperedges is called the hyperdegree of nodes, which is represented by k. The number of nodes in the hyperedge becomes the cardinal number of the hyperedge, which is represented by m. If the cardinal size of all hyperedges in the hypergraph is the same and $m = 2$, the hypergraph is reduced to a simple graph, and the definition of hyperdegree is simplified to that of degree (Battiston et al., 2020).

Considering the higher-order interaction of networks, the field of hypergraph has attracted extensive attention from scientists. In 2021, Sun and Bianconi (2021) studied the cascading failures

[*] Corresponding author.
E-mail addresses: wwzqbx@hotmail.com, wwzqbc@cqmu.edu.cn (W. Wang).

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2022.04.017
1319-1578/

process of nodes after random failure in single-layer and multi-layer random hypergraph networks based on the random attack on hypergraph and successfully derived the theoretical formula. The percolation process on the hypergraph under random failure is revealed. Previously, a large number of experiments have proved that in simple networks, targeted attacks are more destructive to the network than random attacks. Is this the same in hypergraph networks? Based on this, we are committed to studying how the network robustness changes under the target attack based on the size of hyperedge's cardinality in random hypergraph networks.

This paper provides a framework for thoroughly analyzing the resilience of random hypergraph networks against target attacks based on the magnitude of hyperedge's cardinality. Our framework can predict the threshold point of state transition from steady-state to broken-state. We find that similar to the random failure case, the targeted attack on the random hypergraph also shows a second-order phase transition (Parshani et al., 2010). The contributions are as follows:

- Compared with the research of random failure in hypergraph networks, we first propose a target attack strategy based on the size of hyperedge's cardinality. Through mathematical derivation, we get a strict theoretical framework. The effectiveness and correctness of the framework are verified in the simulation. We can conclude that the robustness of the network is more vulnerable with the increase of the probability that the hyperedge with large cardinality is removed.
- Similar to the conclusion that the targeted attacks is more destructive to the simple network than the random attacks, we also found that in the hypergraph network, attacking those hyperedges with large cardinality makes the network collapse faster than randomly removing the hyperedges.
- We have carried out experiments on artificial hypergraph network, and it can be found that our theoretical derivation results are consistent with the experimental simulation results. In addition, we find that the phase transition caused by targeted attacks is also a second-order phase transition, just as the cascading failures of hypergraph network caused by random attacks.

2. Related works

We will mostly discuss node-based and edge-based attacks in this section.

2.1. Node-based-attacks

The percolation problem is to analyze the relationship between the giant connected cluster (GCC) and node (or edge) occupancy probability p after removing $(1-p)$ fraction nodes (or edges). Node-based attacks are often inseparable from the site percolation model. There are two selection methods for removing nodes: random selection removal (random attack), and selection removal according to the attributes of nodes (target attack).

For random attacks, as early as 2000, Callaway et al. (2000) found that the reciprocal of the network average degree is equal to the phase transition point of percolation by constructing an Erdös-Rényi (ER) random network. However, Cohen et al. (2011) found that almost all nodes need to be removed to make the Scale-Free (SF) network collapse ultimately. Therefore, it is concluded that the network has strong robustness against random attacks. In 2010, the research of Buldyrev et al. (2010) was of great significance, shifting researchers' attention from the previous research of single-layer networks to the research of multi-layer networks. It finds the threshold of random attack in multi-layer interdependent networks and obtains its robustness under certain conditions. With time development, 2021 is also a year of great significance. Different from the above simple networks, Sun and Bianconi (2021) began to study the robustness of hypergraph networks with higher-order interaction against random attacks and established a mathematical framework.

Because the difference in node degree in an ER random network is not very visible when the target attacks the single-layer network, the effect of the node with a high-degree target attack is not very significant. However, in the SF network, due to the significant difference of node degree values, Cohen et al. (2001) found that the network can collapse as long as several central nodes in the network are removed.

After 2010, even though we know that high-degree nodes may have a significant influence on the resilience of single-layer networks, Huang et al. (2011) discovered that changing the robustness of networks by attacking high-degree nodes in interdependent networks is challenging. In 2021, different from target attacks in undirected networks, Xu et al. (2021) studied the robustness of relying on directed networks to deal with target attacks on high- or low-degree nodes.

2.2. Edge-based-attacks

In real life, we can effectively protect important nodes, such as power stations, but it is challenging to protect edges, such as transmission lines. Therefore, the research on edge attacks is more meaningful, and the research on bond percolation is edge-based-attack. Compared with random edge removal, target attack edge is more likely to lead to network collapse.

As early as 2000, Moore and Newman (2000) investigated the bond percolation problem on one-dimensional small-world networks using the disease transmission problem as a model. Newman et al. (2002) went on to investigate the bond percolation problem in two-dimensional small-world networks later. Li et al. (2012) revealed in detail the cascading failures process of different classical networks (ER, SF, WS networks) under the strategy of removing the highest-load edges. Unlike the classic method of deliberately selecting the edge with the highest-load for removal, Wang and Rong (2011) proposed two new edge-based-attack strategies (choose the edge with the lowest-load and the edge with a minor ratio of neighboring edges' total capacity to the capacity of the attacked edge) to study the resilience of the United States' western power grid. Hackett et al. (2016) studied the problem of bond percolation on multi-layer networks in detail. Wang et al. (2018) mainly discussed how SF networks respond to two different edge-based-attack, that is, removing edges by ascending or descending order of the loads. Different from the usual definition of edge load by the degree or the betweenness, Hao et al. (2020) defined the initial load on edge using harmonic closeness and then attacked the edge based on this definition to analyze the network's robustness. Other researchers use edge removal strategy to minimize the transmission range of infectious diseases or to study the robustness of network (Yang et al., 2013; Nie et al., 2014; Wang and Liu, 2017).

The above edge attacks are carried out on simple networks with pairwise interaction. However, in the research in 2021, Jhun (2021) studied effective epidemic control strategies in hypergraph networks, including immunization against hyperedges with high simultaneous infection probability.

3. Preliminaries and theoretical framework

Since the number of nodes that can be included in the hyperedge is greater than or equal to 2, in order to facilitate the calculation of the distribution of hyperedge's cardinality in theoretical derivation. We apply the idea of transforming hypergraph into a factor graph to tackle the dynamic problem in response to targeted attacks. We abstract the hyperedge into the corresponding factor node, and calculate its degree according to the number of nodes connected with it, so as to calculate the degree distribution of the hyperedge's cardinality. For details, refer to Sun and Bianconi (2021). At the moment, the essence of a factor graph is a bipartite graph made up of nodes and factor nodes. The targeted attack on the hyperedge in the hypergraph is equivalent to the targeted attack on the factor node in the factor graph. When the hyperedge is removed, the higher-order interaction between the nodes contained in the hyperedge disappears. Some nodes may lose their connectivity with the network, which significantly impacts the robustness of the network. Fig. 1 illustrates the transformation of a hypergraph into its corresponding factor graph.

In addition, it is worth noting that although hyperedges can be included in hyperedges when constructing a random hypergraph, because hyperedges randomly include nodes, when node v_i and node v_j are known to exist in a hyperedge e_i at the same time, the likelihood that node v_i and node v_j exist in another hyperedge e_j at the same time tends to 0, and when N tends to infinity. Similarly, the probability that three or more nodes exist on two different hyperedges at the same time will tend to 0 exponentially (Buldyrev et al., 2010). As a result, the factor graph matching to the random hypergraph has a locally tree-like topology, implying no so-called "circle". To begin, give each factor node a $\Omega_\beta(m_i)$ value to represent the inactivation probability of the factor node e_i, where m_i represents the number of nodes included in hyperedge e_i, that is, the size of hyperedge. To prevent the occurrence of singularities, we use (m_i+1) (Gallos et al., 2005), the function family is obtained

$$\Omega_\beta(m_i) = (m_i+1)^\beta * \left[\sum_{i=1}^{N'}(m_i+1)^\beta\right]^{-1}, -\infty < \beta < +\infty. \tag{1}$$

where N' is the total number of hyperedges, it is not difficult to consider several obvious situations. When $\beta > 0$, the larger the size of the hyperedge, the easier it is to be removed. When $\beta < 0$, the smaller the size of the hyperedge, the easier it is to be removed. When β = 0, $\Omega_0 = 1/N'$, indicates that the hyperedge is removed randomly. When $\beta \to \infty$, it indicates that hyperedges are removed in strict order of size from large to small (as shown in Fig. 2).

Next, the derivation process of the theoretical framework we use is introduced in detail. In the factor graph, the generating function of the node's degree distribution is defined as

$$\psi_0(x) \equiv \sum_k P(k)x^k. \tag{2}$$

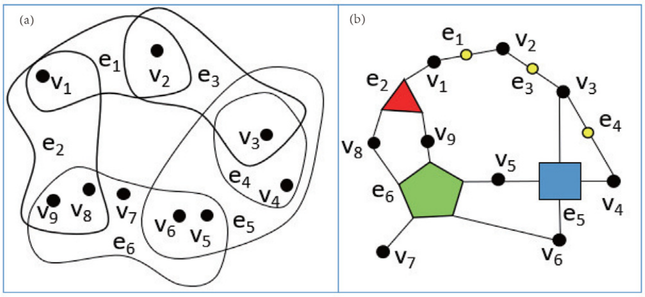

Fig. 1. The figure is a schematic diagram of transforming a hypergraph into a factor graph. The hypergraph comprises nine nodes and six hyperedges (panel (a)). Panel (b) is the factor graph corresponding to the hypergraph. The black dot represents the node, and the yellow dot, red triangle, blue square, and green pentagon represent the hyperedges with a cardinality 2, 3, 4, and 5, respectively.

where $P(k)$ denotes the node's degree distribution. (k is actually expressed as the hyperdegree in the hypergraph), and the excess degree distribution's generating function is

$$\psi_1(x) = \frac{\psi_0'(x)}{\psi_0'(1)}. \tag{3}$$

The generating function of the factor node's degree distribution is defined as

$$\bar{\psi}_0(x) \equiv \sum_m \widehat{P}(m)x^m. \tag{4}$$

where $\widehat{P}(m)$ denotes the factor node's degree distribution (m is actually expressed as the size of the hyperedge in the hypergraph), and the excess degree distribution's generating function is

$$\bar{\psi}_1(x) = \frac{\bar{\psi}_0'(x)}{\bar{\psi}_0'(1)}. \tag{5}$$

Assume that each factor node gets deleted at random with a percentage of $(1-p)$, Sun and Bianconi (2021) define the likelihood of reaching a factor node belonging to the GCC from a node along with the edge as $\hat{s}$, the likelihood of reaching a node belonging to the GCC from a factor node along the edge as s, as shown in Fig. 3. The self-consistent equations (Feng et al., 2015) of s and $\hat{s}$ are:

$$\begin{aligned} \hat{s} &= p\sum_m \tfrac{m}{\langle m\rangle}\widehat{P}(m)\left[1-(1-s)^{m-1}\right], \\ s &= \sum_k \tfrac{k}{\langle k\rangle}P(k)\left[1-(1-\hat{s})^{k-1}\right]. \end{aligned} \tag{6}$$

The order parameter R expresses the ratio of GCC size to initial network size in steady-state, and R can be solved by $\hat{s}$

$$R = 1 - \sum_k P(k)(1-\hat{s})^k \tag{7}$$

Our goal is to turn the hypergraph's target attack problem into a random attack problem that can be solved using the equation above. According to the Eqs. (2)–(5), the Eqs. (6) and (7) can be transformed into

$$\begin{aligned} \hat{s} &= p\left(1-\bar{\psi}_1(1-s)\right), \\ s &= \left(1-\psi_1(1-\hat{s})\right). \end{aligned} \tag{8}$$

and

$$R = 1 - \psi_0(1-\hat{s})\} \tag{9}$$

The bottleneck of hypergraph network research lies in the lack of more novel mathematical tools. However, there are many articles on target attacks against node degrees on simple networks, which also brings some inspiration to our work (Han et al., 2021; Dong et al., 2012; Dong et al., 2013). We initially try to find the relationship between the cardinality of hyperedge and node degrees and try to solve our problem (as shown in Fig. 4). Unfortunately, this problem has not been solved. Nevertheless, there are also unexpected gains. During the experiment, we found that the degree distribution of nodes is in proportion to the distribution of the cardinality of the hyperedge, which is related to the size of the average hyperdegree, as shown in Fig. 5 (a)-(c).

Since the nodes and factor nodes are randomly connected, it is not difficult to imagine that the degree distribution of the factor node after the mapping and the degree distribution before the mapping should also be proportional when the average hyperdegree is certain (as shown in Fig. 6). For the sake of the preciseness

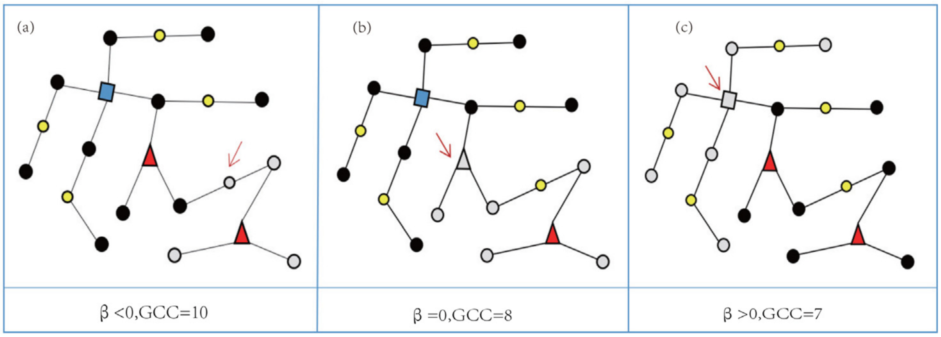

Fig. 2. The factor graph comprises thirteen nodes and eight factor nodes. Panels (a), (b), and (c) are schematic diagrams of the size of GCC in the network when β is less than, equal to or greater than 0, respectively. We can see that with the increase of β, the probability of removing factor nodes with large degree is also increasing, and the size of GCC in the network is becoming smaller and smaller.

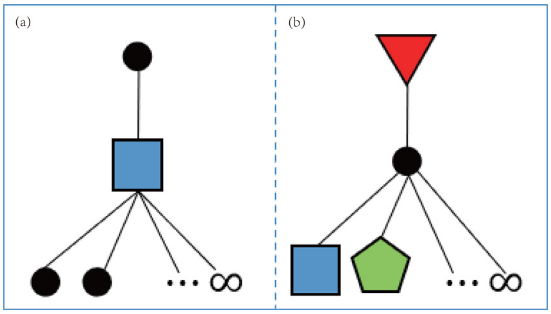

Fig. 3. Panels (a) and (b) depict $\hat{s}$ and s, respectively. A node is in GCC if it is connected to a factor node and at least one of the other nodes connected to the factor node is in GGC. When a factor node is connected to a node and at least one of the other factor nodes connected to the node is in GGC, the factor node is in GCC as well.

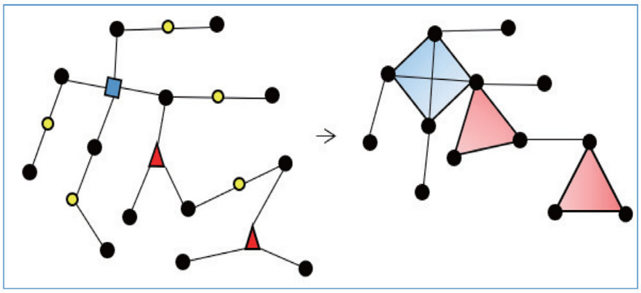

Fig. 4. The graph describes the relationship between the cardinality of the hyperedge and the node degree. The factor node provides a path for the nodes connected to it, thus affecting its degree. It is not difficult to see that the degree of a node has a certain relationship with the size of the hyperedge's cardinality connected by the node.

of scientific research, we also conducted experiments, and the experimental results confirmed our conjecture, as shown in Fig. 5(d)-(f). If two-factor nodes are connected to the same node in the factor graph, that node acts as a bridge, providing a path for the two-factor nodes; it can be regarded as two-factor nodes connected because the node has never been deleted in a targeted attack, knowing this is very helpful for us to solve the problem.

In a network composed of only factor nodes, according to the Eq. (1), after deleting the $(1-p)$percentage of factor nodes from the network, calculate the degree distribution $A_p(m)$ of the not-deleted factor nodes while preserving the edges of the not-deleted factor nodes that connect to the deleted factor nodes. Define $\psi_p(m)$ as the number of factor nodes with degree m,

$$A_p(m) = \frac{\psi_p(m)}{pN'}. \tag{10}$$

When another node is deleted, $A_p(m)$ changes as follows:

$$\psi_{(p-1/N')}(m) = \psi_p(m) - \frac{A_p(m)(m+1)^\beta}{\sum_m A_p(m)(m+1)^\beta}, \tag{11}$$

When $N' \to \infty$, the Eq. (11) may be written as the derivative of $\psi_p(m)$ with regard to p, and p is differentiated in Eq. (10), we can get

$$-p\frac{d\psi_p(m)}{dp} = A_p(m) - \frac{A_p(m)(m+1)^\beta}{\sum_m A_p(m)(m+1)^\beta}, \tag{12}$$

this is correct for $N' \to \infty$. To solve Eq. (12), we establish a function $\psi_\beta(x) \equiv \sum_m P(m)x^{(m+1)^\beta}$, and then, following Shao et al. (2009), create a new parameter $t \equiv \psi_\beta^{-1}(p)$.

$$p = \psi_\beta(t) \equiv \sum_m P(m)t^{(m+1)^\beta}. \tag{13}$$

We discover that the solution to Eq. (12) is

$$A_p(m) = P(m)\frac{t^{(m+1)^\beta}}{\psi_\beta(t)} = \frac{1}{p}P(m)t^{(m+1)^\beta}, \tag{14}$$

and

$$\sum_m A_p(m)(m+1)^\beta = \frac{t\psi'_\beta(t)}{\psi_\beta(t)}. \tag{15}$$

this can be demonstrated to fulfill Eq. (12). After deleting a percentage $(1-p)$ of the factor nodes from the network using Eq. (1), the generating function of the factor nodes that remain in the network is

$$\psi_b(x) \equiv \sum_m A_p(m)x^m = \frac{1}{p}\sum_m P(m)t^{(m+1)^\beta}x^m, \tag{16}$$

Because the factor nodes are connected at random, the likelihood that an edge will terminate at a not-deleted factor node is equal to the ratio of the number of edges starting from not-deleted factor nodes to the total number of edges starting from all the factor nodes in the original network:

$$\tilde{p} \equiv \frac{pN'\langle m(p)\rangle}{N'\langle m\rangle} = \frac{\sum_m P(m)mt^{(m+1)^\beta}}{\sum_m P(m)m}. \tag{17}$$

where the average degree of the remaining nodes is $\langle m(p)\rangle = \sum_m A_p(m)m$. Deleting the edges of a randomly connected

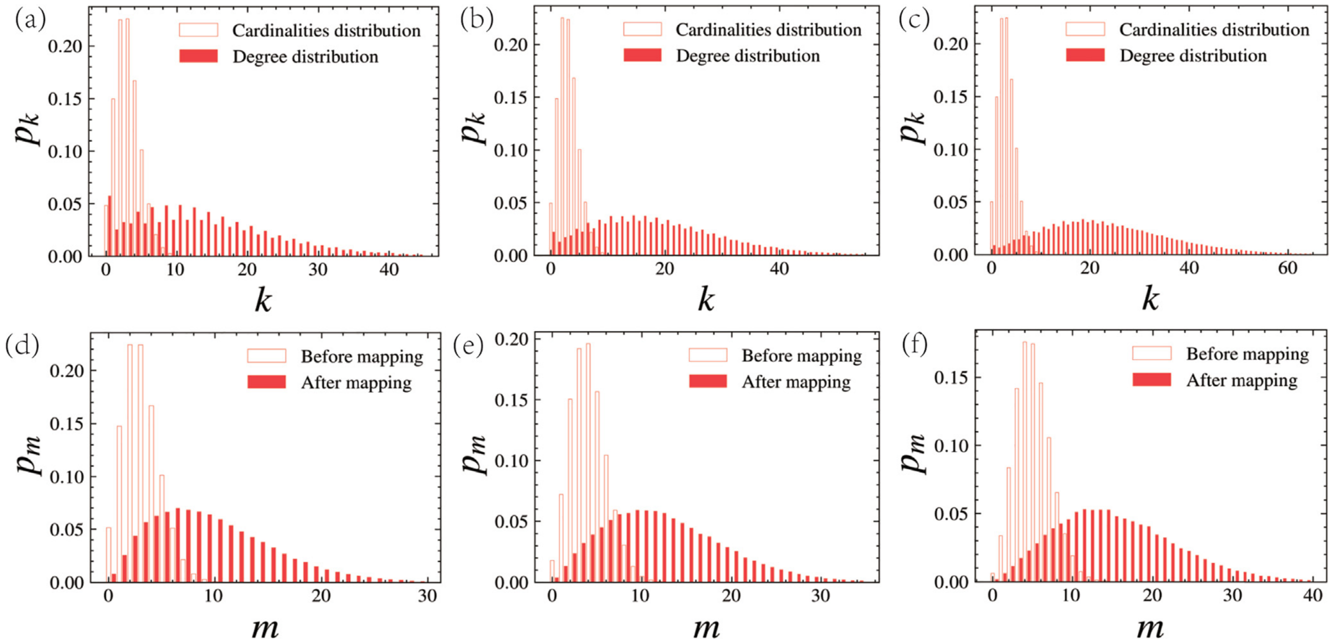

Fig. 5. Based on the random hypergraph network with $\left(N = 10^5\right)$ nodes whose hyperdegree distribution and hyperedge's cardinality distribution meet Poisson distribution, panels (a)-(c) is fixed expectation ($\langle m \rangle = 3$) and set expectation $\langle k \rangle$ = 3, 4 and 5 respectively. It can be seen that the cardinality distribution and degree distribution are more widely distributed in a certain proportion with the increase of $\langle k \rangle$. Panels (d)-(f) is fixed expectation ($\langle k \rangle = 3$), and set expectation $\langle m \rangle$ = 3, 4 and 5 respectively. It can be seen that the degree distribution after the mapping of factor node is in a certain proportion to the degree distribution before the mapping, and the distribution is wider with the increase of $\langle m \rangle$. Note that the abscissa k and m here represent different meanings under different backgrounds.

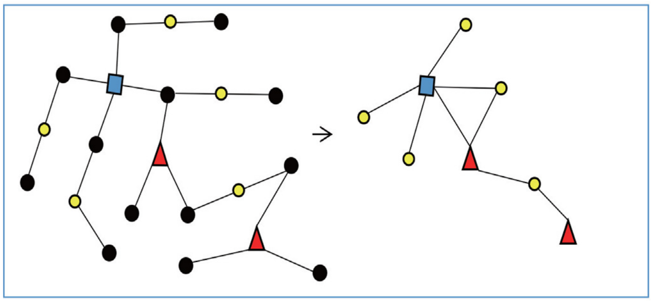

Fig. 6. This figure describes the relationship between the degree of factor nodes before and after mapping. The node provides a path for the factor node connected to it, which affects the degree of the changed factor node. It is not difficult to see that the degree of the factor node after the mapping has a specific relationship with the degree of the factor node before the mapping.

network that terminate at the deleted factor nodes is equal to randomly deleting a $(1 - \tilde{p})$ percentage of the not-deleted factor nodes' edges. And use the same strategy as in Newman (2002), it is possible to demonstrate that the not-deleted factor node's generating function after random removal of $(1 - \tilde{p})$ percentage of edges equals

$$\psi_c(x) \equiv \psi_b(1 - \tilde{p} + \tilde{p}x), \tag{18}$$

We can acquire the following relationship if we can discover a network $\bar{\psi}_{eq}$ with generation function $\bar{\psi}_{eq0}(x)$, such that after randomly deleting the factor nodes of percentage $(1 - p)$, that

$$\bar{\psi}_{eq0}(x) = \psi_c(1 - p + px), \tag{19}$$

We may derive the following conclusion via Eqs. (18) and (19)

$$\bar{\psi}_{eq0}(x) = \psi_b\left(1 - \frac{\tilde{p}}{p} + \frac{\tilde{p}}{p}x\right), \tag{20}$$

The excess degree distribution's generating function is

$$\bar{\psi}_{eq1}(x) = \frac{\psi'_{eq0}(x)}{\psi'_{eq0}(1)}. \tag{21}$$

Since the node has never been deleted from beginning to end, in the self-consistent equations, the generating function of the hyperdegree remains unchanged. However, the equivalent generating function of the hyperedge's cardinalities distribution and the excess hyperedge's cardinalities distribution after the targeted attack satisfies the Eqs. (20) and (21). Therefore, the target attack problem on hypergraph networks based on the size of the hyperedge can be mapped to the random attack problem on hypergraph networks.

According to the Eqs. (8) and (21), we can get the self-consistent equations of the equivalent network of hypergraph network under target attack as

$$\begin{aligned} \hat{s} &= p\left(1 - \bar{\psi}_{eq1}(1 - s)\right), \\ s &= (1 - \psi_1(1 - \hat{s})). \end{aligned} \tag{22}$$

the order parameter R is

$$R = 1 - \psi_0(1 - \hat{s}). \tag{23}$$

4. Experiment

To comprehend the impact of various hyperedge removal strategies on the robustness of hypergraph networks, Monte-Carlo simulation (Newman and Ziff, 2000) experiments were carried out on artificial hypergraph networks. On the premise of different β values, we carried out experiments on different hyperdegree distributions and hyperedge's cardinality distributions on artificial hypergraph networks with fixed network scale (Newman et al., 2001).

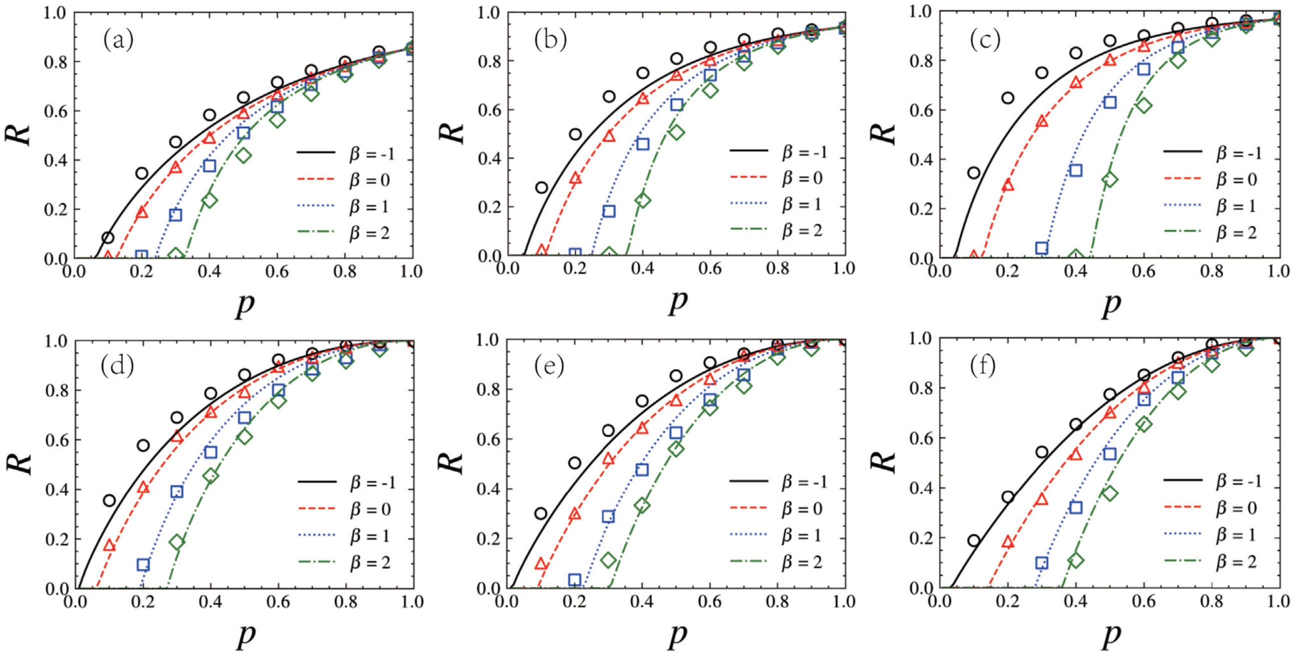

Fig. 7. Panels (a), (b) and (c) represent different values of β under $(\langle k\rangle = 2, \langle m\rangle = 4); (\langle k\rangle = 3, \langle m\rangle = 3)$ and $(\langle k\rangle = 4, \langle m\rangle = 2)$ $(N = 10^4)$. Panels (d), (e) and (f) represent different values $\lambda_k = \lambda_m$ = 2.6, 3.0 and 3.5 $(N = 2 * 10^2)$. The smooth curve represents the theoretical solution derived from mathematics, and the symbol represents the simulation results in synthetic random hypergraph network. It is not difficult to find that the two agree well.

For simplicity, in the first case, we obey Poisson distribution for both hyperdegree distribution and hyperedge's cardinality distribution, that is,

$$P\left(\tilde{k}\right) = \left[e^{-\langle\tilde{k}\rangle} * \left\langle\tilde{k}\right\rangle^{\tilde{k}} / \tilde{k}!\right], \tag{24}$$

where $\tilde{k}$ represents the degree of node, $\left\langle\tilde{k}\right\rangle$ represents the average degree, also known as mathematical expectation.

Next, in a random hypergraph network with N nodes, we make $\langle k\rangle$ and $\langle m\rangle$ meet different expectations respectively. At this point, the number of hyperedges N' is $(N * \langle k\rangle / \langle m\rangle)$.

On a hypergraph network with a certain number of nodes $(N = 10^4)$ whose the hyperdegree distribution and the cardinality of hyperedge distribution obey Poisson distribution, we make $\langle k\rangle$ and $\langle m\rangle$ meet $\langle k\rangle = 2, \langle m\rangle = 4; \langle k\rangle = 3, \langle m\rangle = 3$and $\langle k\rangle = 4, \langle m\rangle = 2$respectively. And we set parameter β to - 1, 0, 1 and 2 respectively. It is worth noting that when β takes 0, the target attack problem is equivalent to the random attack problem. Because the larger the value of β is, the greater the probability that the hyperedge with large cardinality will be removed. The experimental findings reveal that the random hypergraph network becomes more fragile as the probability of removing hyperedges with large cardinality increases, as shown in Fig. 7 (a) - (c).

In the second case, we obey power-law distribution for both hyperdegree distribution and hyperedge's cardinality distribution, that is,

$$P\left(\tilde{k}\right) = \left[\left(\tilde{k}+1\right)^{1-\lambda} - \tilde{k}^{1-\lambda}\right] / \left[\left(\widetilde{M}+1\right)^{1-\lambda} - \tilde{m}^{1-\lambda}\right], \tag{25}$$

Where $\tilde{k}$ represents the degree of node, $\widetilde{M}$ represents the maximum degree, $\tilde{m}$ represents the minimum degree.

For simplicity, we set the exponent λ of two groups of nodes in the Eq. (25) to be the same ($\lambda_k = \lambda_m$ = 2.6, 3.0 and 3.5), the $\widetilde{M}_k = \widetilde{M}_m = \sqrt{N}$, the $\tilde{m}_k = \tilde{m}_m = 2$, and then we construct a random hypergraph network with $(N = 2 * 10^2)$ nodes. At this point, the number of hyperedges N' is set to be the same as the number of nodes N. Experiments with various exponent values are carried out, the results also reveal that the higher the likelihood of deleting a large-size hyperedge, the faster the hypergraph network collapses, as shown in Fig. 7 (d) - (f). Each of the experiments was repeated ten times, and the final result was an average of ten times. All the experiments were performed on a personal computer with 4G memory and 2.50 GHz Intel i5-7200U CPU.

5. Conclusions and discussion

This study first investigates the resilience of hyperedge's cardinality distribution and random hypergraph using a mathematical framework dependent on the size of hyperedge's cardinality. Our framework can well analyze the changes in the robustness of hypergraph networks against target attacks. Firstly, in the dynamic process, we demonstrate the impact of the random attack $(\beta = 0)$ and target attack $(\beta \neq 0)$ on the reliability of the hypergraph network. It is found that a targeted attack $(\beta > 0)$ is easier to affect the reliability of the network and cause more node failures than a random attack.

In order to facilitate the calculation, we model the hypergraph network as a factor graph. Factor graphs are associated with hypergraphs through simple mapping. On this basis, we obtain the hyperedge's cardinality distribution. The self-consistent equations are introduced in the theoretical derivation, and the theoretical formula of target attack based on hyperedge's cardinality is derived. Then the relationship between different target attack strategies (i.e. β takes different values) and the resilience of hypergraph network is obtained.

Our experiment is carried out when the basic structure of the hypergraph network is the hyperdegree, and the cardinality of hyperedge obeys Poisson distribution, the hyperdegree, and the cardinality of hyperedge obeys the power-law distribution to verify the validity of these equations proposed under various topological structures. Consistent with the conclusions of previous papers on target attacks, a targeted attack is more destructive to the network than a random attack. We find that for a single-layer random hypergraph network, for any targeted attack with β value, the phase transition shows a second-order phase transition. Furthermore, when the value of β increases, the probability of removing the hyperedge with large cardinality increases; that is, the threshold point of state transition of the network also increases, and the system becomes more vulnerable. Our theoretical framework can accurately find the threshold points of random hypergraph networks in a targeted attack; these findings can help us understand the impact of the underlying structure of hypergraph networks on their robustness.

CRediT authorship contribution statement

Hao Peng: Funding acquisition, Conceptualization, Methodology, Project administration. **Cheng Qian:** Software, Validation, Formal analysis. **Dandan Zhao:** Writing - review & editing, Supervision. **Ming Zhong:** Writing - original draft. **Xianwen Ling:** Investigation. **Wei Wang:** Funding acquisition, Conceptualization.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

We acknowledge the National Natural Science Foundation of China (62072412, 61902359, 61702148, and 61672468), the Opening Project of Shanghai Key Laboratory of Integrated Administration Technologies for Information Security (AGK2018001), and the Natural Science Foundation of Chongqing (cstc2021jcyj-msxmX0132).

References

Alotaibi, N., Rhouma, D., 2021. A review on community structures detection in time evolving social networks. J. King Saud University-Computer Inform. Sci.

Battiston, F., Cencetti, G., Iacopini, I., Latora, V., Lucas, M., Patania, A., Young, J.-G., Petri, G., 2020. Networks beyond pairwise interactions: structure and dynamics. Phys. Rep. 874, 1–92.

Berahmand, K., Nasiri, E., Forouzandeh, S., Li, Y., 2021. A preference random walk algorithm for link prediction through mutual influence nodes in complex networks. J. King Saud University-Computer Inform. Sci.

Bondy, J.A., Murty, U.S.R., et al., 1976. Graph theory with applications, volume 290. Macmillan, London.

Bretto, A., 2013. Hypergraph theory, An introduction. Mathematical Engineering. Springer, Cham.

Buldyrev, S.V., Parshani, R., Paul, G., Stanley, H.E., Havlin, S., 2010. Catastrophic cascade of failures in interdependent networks. Nature 464, 1025–1028.

Callaway, D.S., Newman, M.E., Strogatz, S.H., Watts, D.J., 2000. Network robustness and fragility: Percolation on random graphs. Phys. Rev. letters 85, 5468.

Cohen, R., Havlin, S., 2010. Complex networks: structure, robustness and function. Cambridge University Press.

Cohen, R., Erez, K., Ben-Avraham, D., Havlin, S., 2001. Breakdown of the internet under intentional attack. Phys. Rev. Letters 86, 3682.

Cohen, R., Erez, K., Havlinl, S., Newman, M., Barabási, A.-L., Watts, D.J., et al., 2011. Resilience of the internet to random breakdowns. In: The Structure and Dynamics of Networks. Princeton University Press, pp. 507–509.

Dong, G., Gao, J., Tian, L., Du, R., He, Y., 2012. Percolation of partially interdependent networks under targeted attack. Phys. Rev. E 85, 016112.

Dong, G., Gao, J., Du, R., Tian, L., Stanley, H.E., Havlin, S., 2013. Robustness of network of networks under targeted attack. Phys. Rev. E 87, 052804.

Feng, L., Monterola, C.P., Hu, Y., 2015. The simplified self-consistent probabilities method for percolation and its application to interdependent networks. New J. Phys. 17, 063025.

Gallos, L.K., Cohen, R., Argyrakis, P., Bunde, A., Havlin, S., 2005. Stability and topology of scale-free networks under attack and defense strategies. Phys. Rev. Letters 94, 188701.

Ghoshal, G., Zlatić, V., Caldarelli, G., Newman, M.E., 2009. Random hypergraphs and their applications. Phys. Rev. E 79, 066118.

Hackett, A., Cellai, D., Gómez, S., Arenas, A., Gleeson, J.P., 2016. Bond percolation on multiplex networks. Phys. Rev. X 6, 021002.

Han, J., Tang, S., Shi, Y., Zhao, L., Li, J., 2021. An efficient layer node attack strategy to dismantle large multiplex networks, The. Eur. Phys. J. B 94, 1–8.

Hao, Y., Wang, Y., Jia, L., He, Z., 2020. Cascading failures in networks with the harmonic closeness under edge attack strategies. Chaos, Solitons & Fractals 135, 109772.

Huang, X., Gao, J., Buldyrev, S.V., Havlin, S., Stanley, H.E., 2011. Robustness of interdependent networks under targeted attack. Phys. Rev. E 83, 065101.

Jhun, B., 2021. Effective epidemic containment strategy in hypergraphs. Phys. Rev. Res. 3, 033282.

Li, S., Li, L., Yang, Y., Luo, Q., 2012. Revealing the process of edge-based-attack cascading failures. Nonlinear Dyn. 69, 837–845.

Li, W., Xue, X., Pan, L., Lin, T., Wang, W., 2022. Competing spreading dynamics in simplicial complex. Appl. Math. Comput. 412, 126595.

Moore, C., Newman, M.E., 2000. Epidemics and percolation in small-world networks. Phys. Rev. E 61, 5678.

Newman, M.E., 2002. Spread of epidemic disease on networks. Phys. Rev. E 66, 016128.

Newman, M.E.J., 2010. Networks: An Introduction. Oxford University Press.

Newman, M., Ziff, R.M., 2000. Efficient monte carlo algorithm and high-precision results for percolation. Phys. Rev. Lett. 85, 4104.

Newman, M.E., Strogatz, S.H., Watts, D.J., 2001. Random graphs with arbitrary degree distributions and their applications. Phys. Rev. E 64, 026118.

Newman, M.E., Jensen, I., Ziff, R., 2002. Percolation and epidemics in a two-dimensional small world. Phys. Rev. E 65, 021904.

Nie, S., Wang, X., Zhang, H., Li, Q., Wang, B., 2014. Robustness of controllability for networks based on edge-attack. PloS one 9, e89066.

Parshani, R., Buldyrev, S.V., Havlin, S., 2010. Interdependent networks: Reducing the coupling strength leads to a change from a first to second order percolation transition. Phys. Rev. Letters 105, 048701.

Peng, H., Peng, W., Zhao, D., Wang, W., 2020. Impact of the heterogeneity of adoption thresholds on behavior spreading in complex networks. Appl. Math. Comput. 386, 125504.

Shao, J., Buldyrev, S.V., Braunstein, L.A., Havlin, S., Stanley, H.E., 2009. Structure of shells in complex networks. Phys. Rev. E 80, 036105.

Singh, S.S., Srivastva, D., Verma, M., Singh, J., 2021. Influence maximization frameworks, performance, challenges and directions on social network: A theoretical study. J. King Saud University-Computer Inform. Sci.

Sun, H., Bianconi, G., 2021. Higher-order percolation processes on multiplex hypergraphs. Phys. Rev. E 104, 034306.

Wang, S., Liu, J., 2017. Enhancing the robustness of complex networks against edge-based-attack cascading failures. In: 2017 IEEE Congress on Evolutionary Computation (CEC). IEEE, pp. 23–28.

Wang, J.-W., Rong, L.-L., 2011. Robustness of the western united states power grid under edge attack strategies due to cascading failures. Safety Sci. 49, 807–812.

Wang, Z., Zhou, D., Hu, Y., 2018. Group percolation in interdependent networks. Phys. Rev. E 97, 032306.

Wang, Y., Cao, J., Li, X., Alsaedi, A., 2018. Edge-based epidemic dynamics with multiple routes of transmission on random networks. Nonlinear Dyn. 91, 403–420.

Xu, W., Pan, L., Liu, X., 2021. Breakdown in interdependent directed networks under targeted attacks. EPL (Europhysics Letters) 133, 68004.

Yang, H.-X., Wu, Z.-X., Wang, B.-H., 2013. Suppressing traffic-driven epidemic spreading by edge-removal strategies. Phys. Rev. E 87, 064801.

Zhao, D., Li, R., Peng, H., Zhong, M., Wang, W., 2022. Higher-order percolation in simplicial complexes. Chaos, Solitons & Fractals 155, 111701.

Zhou, Z., Jin, Z., Jin, J., Song, H., 2020. Emergence of scaling in evolving hypernetworks. Physica A 546, 123765.