symmetry

MDPI

Article

Study on the Cascading Failure Robustness of the Belt and Road Land–Sea Transport Network under Emergencies

Chaojun Ding *, Zhilin Wang and Susu Xu

School of Naval Architecture and Maritime, Zhejiang Ocean University, Zhoushan 316022, China; wangzhilin@zjou.edu.cn (Z.W.); xususu@zjou.edu.cn (S.X.)
* Correspondence: dingchaojun@zjou.edu.cn; Tel.: +86-178-5880-7599

Abstract: When studying an unfamiliar system, we first look for the symmetry that the system has so that we can make many predictions about the possible properties of the system. The symmetry in transport network security needs to maintain a stable state and maintain a constant state of transport network security. With the development of China–Europe freight trains, the transport between Asia and Europe has gradually formed the Belt and Road (B&R) land–sea transport network. In order to analyze the cascading failure mechanism of the B&R land–sea transport network, a network cascading failure model is constructed. Then, the quantitative analysis of the connectivity indicators of the land–sea transport network is conducted from the node attack strategy, and it is compared with the Maritime Silk Road (MSR) shipping network. Finally, the robustness of the land–sea transport network under emergencies is analyzed. From the results of deliberate attacks, the attack threshold of the B&R land–sea transport network is the same as that of the MSR shipping network, and the maximum number of attacks is slightly less than that of the MSR shipping network. The Russia–Ukraine conflict has a minimal impact on the robustness of cascading failure in the land–sea transport network. The Red Sea crisis may have a significant impact on the robustness of cascading failure in the land–sea transport network. The research results can provide suggestions for improving the robustness of the B&R land–sea transport network.

Keywords: the belt and road; land–sea transport network; cascading failure; robustness; emergency

Citation: Ding, C.; Wang, Z.; Xu, S. Study on the Cascading Failure Robustness of the Belt and Road Land–Sea Transport Network under Emergencies. *Symmetry* **2024**, *16*, 736. https://doi.org/10.3390/sym16060736

Academic Editor: Theodore E. Simos

Received: 6 May 2024
Revised: 7 June 2024
Accepted: 11 June 2024
Published: 13 June 2024

1. Introduction

The Belt and Road (B&R) initiative proposed by China involves important international and regional cooperation. Under the B&R initiative, China–Europe freight trains have developed rapidly. According to China Railway data, between January and November 2023, 1.749 million TEU of goods were shipped on China–Europe freight trains, up 19 percent year-on-year [1]. Therefore, land transport is also becoming more and more important in the transportation pattern between Asia and Europe. In this context, to comprehensively analyze the transport pattern between Asia and Europe, we must not only analyze the Suez Canal route, which occupies the dominant position, but also analyze the road transport routes and comprehensively analyze the land–sea transport system of Asia–Europe transport. The Eurasian land–sea transport system can be regarded as a land–sea transport network composed of nodes and routes. In this transport network, each node does not exist in isolation, but develops and evolves in the interactive process with other nodes in the network. With the development of the land–sea transport network, nodes are increasingly interconnected, which increases the vulnerability of the network to disruptions from nodes (such as the closure of the Shanghai port during the COVID-19 pandemic) and routes (Suez Canal blockage, the Red Sea crisis, the change of land routes caused by the Ukraine–Russia conflict, etc.) [2]. Therefore, it is very important to study the robustness of the B&R land–sea transport network.

The research on the risk characteristics such as the robustness of the land–sea transport network is mainly focused on the analysis of the sea transport network and the land

transport network. Among them, the research on the robustness of shipping networks can be summarized in two aspects.

One is to identify key nodes in the shipping network. The importance of the port to the network is reflected in the change in the connectivity of the maritime network after the removal of this node [3–6]. The other is to improve the topology of the shipping network. Different networks have different structures, and different network structures lead to different network robustness [7,8], which can be enhanced by link-rewiring strategies [9] and link-adding strategies [10]. Regarding the robustness of land transport networks, the research objects include urban rail transit networks [11,12] and railway networks [13], and the change in network connectivity when key stations are removed is analyzed.

In addition, the research objects of the B&R transport network are the Maritime Silk Road (MSR) shipping network and the China–Europe freight train network. There are also some studies on the robustness of the MSR shipping network.

For instance, Xie (2019) [14] constructed a maritime network of three cargo ships—container, tanker, and bulk—along the MSR and analyzed the changes in the three networks under different attack strategies. Mou et al. (2020) [15] established the MSR crude oil transport network, studied the impact of network topology and network resilience, and analyzed the changes in resilience of the crude oil transport network under intentional and random attacks. Yang and Liu (2022) [16] used transitivity and diversity to represent the resilience of MSR shipping networks and analyzed the variation characteristics of the resilience by using disruption simulation. With regard to the China–Europe freight train transport network, Lyu et al. (2023) [17] introduced and discussed the ripple effect of the China–Europe freight train transport network.

Current research on transport network robustness generally analyzes network robustness by removing nodes one by one. However, due to the close connection between various nodes in the land–sea transport network, the failure of one node will distribute its cargo flow to nearby nodes, resulting in more nodes being affected or even paralyzed. For instance, at the end of March 2022 due to COVID-19 in Shanghai, the impact of the Shanghai port blockade far exceeded the impact of the Russia–Ukraine war, causing port congestion to spread to other ports and shipping delays at many global hub ports. This phenomenon is called cascade failure, and there have been few studies on the cascade failure robustness of land–sea transport networks, which need to be strengthened.

Due to the importance of cascade failure to many realistic complex systems, research on cascade defense and control strategies to improve network robustness has attracted the interest of several scholars. These scholars have proposed and studied many models for the analysis of network cascading faults, such as the sandpile model [18], the global load-based cascade failure model (GLBCM) [19], and the fiber bundle model [20]. Wang and Chen proposed a local load distribution principle (LWFRR) on weighted networks [21]. Cascading failure models have also been applied to a variety of networks, such as land transportation networks [22], supply chain networks [23], the internet [24], power grids [25], wireless sensor networks [26], and water distribution networks [27]. Xu et al. [28] proposed a new cascading failure model for shipping systems and used it to study global liner shipping networks. At present, there are few studies on the cascade failure of land–sea transportation network. However, with the development of China–Europe freight trains, the transport pattern of Asia and Europe is increasingly showing equal emphasis on land–sea transport, so it is necessary to analyze the cascade failure robustness of the B&R land–sea transport network. In addition, the current cascade failure robustness analysis of the transport network is usually carried out under the assumption of removal points, and the network robustness under real emergencies is rarely analyzed. In this paper, real emergencies such as the Russia–Ukraine conflict and the Red Sea crisis are transformed into changes of network topology, which can provide a basis for the practical application of network robustness theory.

The remainder of this paper is organized as follows. Section 2 introduces the relevant data and methods of the paper. In Section 3, the cascade failure model of the B&R land–sea

transportation network is constructed. The empirical results are presented in Section 4. Section 5 provides the conclusion.

2. Methodology

2.1. Study Areas and Data

First of all, regarding maritime transportation, the data involved in this paper were selected from the relevant shipping route data of the world's top 30 container liner shipping companies provided by Alphaliner, a shipping database, in April 2019. First, according to the website of each shipping company, the corresponding shipping schedules of the liner shipping company were calculated to obtain the ports of call required for ship transportation on each line. To ensure the authenticity of the network, all routes and ports involved in the shipping schedule of the selected liner transport enterprises were counted, and on this basis, the MSR ports extracted. According to the region through which the MSR passes, the MSR includes East Asia, Southeast Asia, South Asia, West Asia, Oceania, Africa, and Europe. Routes through MSR ports are then selected. The method of constructing the network in this paper is the P-space method [29], that is, all ports passing through the container route are connected. The specific construction process is shown in Figure 1.

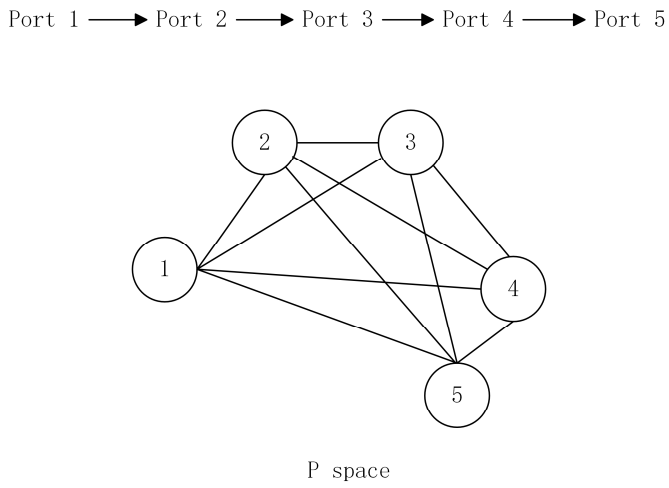


Figure 1. Network Generation.

After processing, an MSR shipping network composed of 594 port nodes and 7333 edges is obtained. The network is shown in Figure 2.

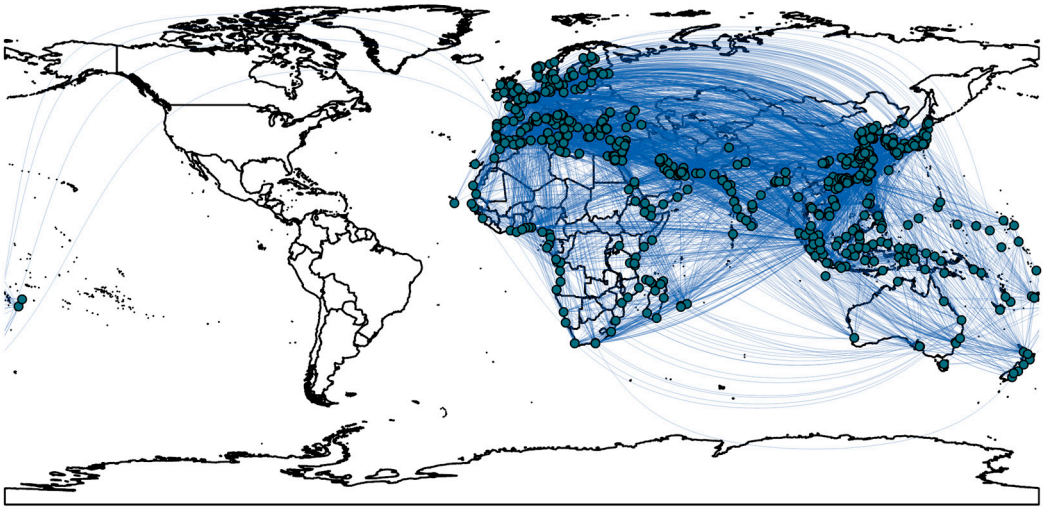


Figure 2. MSR shipping network.

In addition, for the part of land transportation, the relevant data are from the official Chinese website for the Belt and Road Initiative (https://www.yidaiyilu.gov.cn/index.htm, accessed on 1 June 2024), and from the National Railway Freight 95306 Platform of China (http://www.95306.cn/, accessed on 1 June 2024), as well as our own collected data. In this paper, the data of China–Europe freight trains in 2021 are also processed by P-space method. After processing, a China–Europe freight train transport network consisting of 92 node cities and 572 connecting borders is obtained.

Then, the B&R land–sea transport network is obtained by superimposing the MSR shipping network and the China–Europe railway transport network. The resulting land–sea transport network has 664 nodes and 7901 connected edges.

2.2. Network Cascading Failure Model

After the network is constructed, a cascading failure model is established to study its robustness. Under some attack modes, network nodes are redistributed according to the principle of local load distribution. Repeated simulations and evaluations of network destructiveness are performed.

2.2.1. Metrics of Network Complexity

The metrics of network complexity in this paper refer to the research of Freeman [30].

(1) Node degree d_i refers to the number of other nodes in the network that are connected to node i.

$$d_i = \sum_{j=1}^{n} a_{ij} \tag{1}$$

where $a_{ij} = 1$ if there is an edge between node i and node j, $a_{ij} = 0$ if there is no edge between node i and node j.

(2) The betweenness of nodes refers to the probability of all the shortest paths passing through node i in the network, reflecting the transit function of nodes in the network, and the formula is BC_i

$$BC_i = \sum_{j}^{n} \sum_{k}^{h} [N_{jk}(i)/N_{jk}], j \neq k \neq i, j < k \tag{2}$$

where N_{jk} represents the number of shortest paths between node j and node k, and $N_{jk}(i)$ represents the number of two-point shortest paths through i.

(3) Node strength represents the sum of all edge weights adjacent to node i, whose expression is S_i

$$S_i = \sum_{j \in N_i} w_{ij} \tag{3}$$

where w_{ij} represents the weight of node i and the joint edge of node j.

2.2.2. Initial Load and Capacity

The initial load of the node is related to the point strength, assuming that the initial load L_i of the node is equal to the point strength s.

The construction and maintenance of the network are limited by the cost, and the limited network cost should be reasonably allocated to resist cascading failure. The node capacity C_i is calculated as follows:

$$C_i = (1 + \alpha)L_i \tag{4}$$

where α is the tolerance parameter and satisfies $\alpha \geq 0$. With the increase in this parameter, each node has a stronger ability to withstand the impact of the additional distributed load of the failure node in an emergency.

2.2.3. Load-Redistribution

To study the relationship between weighting characteristics and cascade failure, Wang et al. proposed the principle of local load distribution (LWFRR) [21]. When a node fails, its load is redistributed to the corresponding node according to the ratio of the node load in the neighboring domain to the total load of all nodes in the neighboring domain, and the additional load ΔL_{ji} obtained by its neighboring nodes is as follows:

$$\Delta L_{ji} = L_i \cdot C_j^{\beta} / \sum_{m \in \Gamma_i} C_m^{\beta} \tag{5}$$

where L_i is the load of node i, C_j is the load capacity of node j, Γ_i is the neighborhood of node i, C_m is the load of node m, and β is the parameter.

2.2.4. Network Connectivity Indicators

Network robustness refers to the ability of a network to continue to operate after an attack. The robustness indicators selected in this paper include the node retention rate, network efficiency, and giant component size ratio.

(1) The node retention rate R refers to the ratio of the number of retained nodes to the total number of initial network nodes after the initial network is attacked until the network cascade failure node no longer appears. The expression is as follows:

$$R = \frac{N'}{N} \tag{6}$$

where N is the total number of initial network nodes and N' is the total number of nodes retained by the network after the cascade effect.

(2) Network efficiency E reflects the connectivity performance of the network, where efficiency refers to the reciprocal of the shortest path between nodes, and network efficiency is the average of the efficiency between all nodes. The expression is as follows:

$$E = \frac{1}{n(n-1)} \sum_{i \neq j} \frac{1}{d_{ij}} \tag{7}$$

where d_{ij} is the shortest path between node i and node j; when there is no edge between node i and node j, $d_{ij} = +\infty$.

(3) The giant component size ratio C reflects the change in the scale of interconnection after the network is attacked, and the expression is as follows:

$$C = \frac{Z'}{Z} \tag{8}$$

where Z' is the number of nodes with a giant component size after the network is attacked and Z is the initial giant component size.

(4) Node vulnerability and criticality

According to the study of Xu [28], the node vulnerability V_i^{UW} is defined as the average value of the impact of other node failures on the node.

$$V_i^{UW} = \frac{1}{n-1} \sum_{d \in G, d \neq i} \Delta E_i^d \tag{9}$$

where $\Delta E_i^d = \frac{E - E'}{E}$ is the change in node i's efficiency and d is the node initially attacked.

The node criticality C_d^{UW} is the average value of the impact of the initial failure of the node on all other nodes in the network.

$$C_d^{UW} = \frac{1}{n-1} \sum_{i \in G, i \neq d} \Delta E_i^d \tag{10}$$

3. Model Design

3.1. Cascading Failure Algorithm

According to complex network theory, network attacks are generally divided into random attacks and deliberate attacks. In this paper, an attack strategy is designed based on these two kinds of attack methods to simulate the cascading failure process of container networks. The deliberate attack strategy includes the maximum point strength attack strategy, the maximum degree attack strategy, and the maximum betweenness attack strategy. The attack strategy designed in this paper is as follows:

① In the original complex network, a node is selected for attack according to a strategy (random, maximum point strength, maximum degree, and maximum betweenness) each time; that is, the selected node is deleted from the network.

② The load on the node is redistributed according to the local load redistribution principle in the network cascading failure model.

③ If there is an outlier or the load allocated to a node exceeds its capacity, the node is also deleted until the cascading effect stops and the robustness index of the network is calculated.

④ This process is repeated until all the nodes in the network fail.

In addition, the typical external emergencies of the existing B&R land–sea transport network are analyzed. At present, the main geopolitical factors that directly affect the current Asia–Europe transport are the Ukraine–Russia conflict and the Red Sea crisis. Among them, the Russia–Ukraine conflict has some negative effects on China–Europe freight trains. After the outbreak of the crisis in Ukraine, a number of Chinese inland port operators suspended the train service via Ukraine to Poland. Among them, some operators adopt alternative routes, which not only increase the cost, but also increase the transportation time by 3–5 days [31].

In addition, the Red Sea crisis had a greater impact on the Suez Canal route. Since November 2023, Houthi Rebels in Yemen have attacked ships sailing in the Red Sea region, leading to the Red Sea crisis. With the continuation of the Red Sea crisis, it has a negative impact on international shipping in Eurasia [32].

Therefore, this paper transforms these two classical external emergencies into nodes in the network being attacked, and on this basis, carries out the simulation of the network ①–④. The advantages of the attack strategy designed in this paper are as follows: the real emergencies are transformed into network nodes under attack, and the mechanism characteristics of the congestion phenomenon in the B&R land–sea transport network under the emergencies can be analyzed, so as to provide some effective suggestions for improving the cascade failure robustness of the network, which has some practical significance. But this article also has some shortcomings. The research is based on numerical simulation, so the applicability of the model and the setting of parameters appear to be relatively key in the analysis of the cascading failure robustness of the B&R land–sea transport network. For example, whether the parameters port capacity tolerance and local load distribution coefficient are set reasonably will affect whether the cascade failure process of the network is realistic. In addition, the cascade failure model established in this paper may not fully reflect the real situation, and the reliability of the model needs to be further verified.

3.2. Model Process

The model flow of this paper is shown in Figure 3.

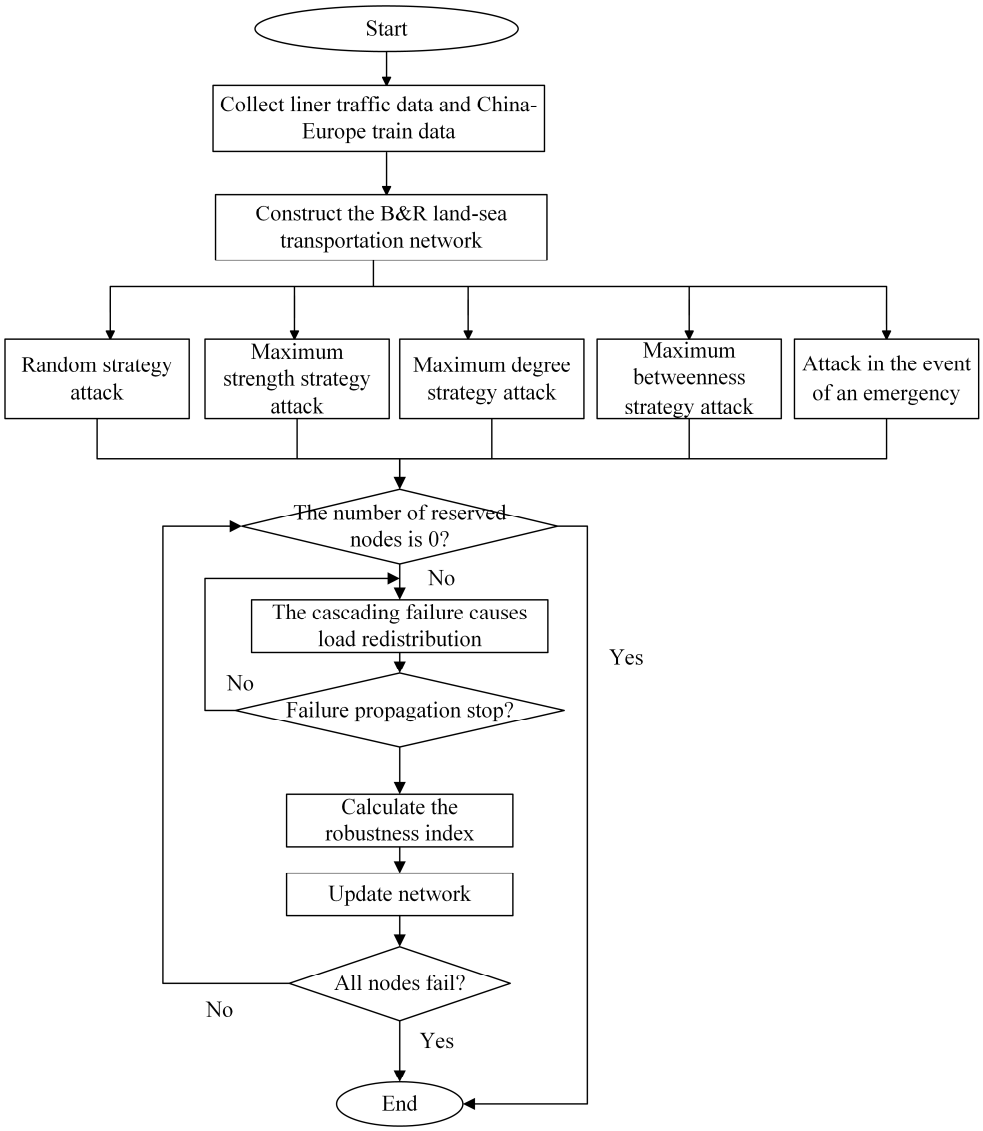


Figure 3. Cascade failure model flow chart of the B&R land–sea transportation network.

4. Results

4.1. Characteristics Analysis of the Belt and Road Land–Sea Transport Network

Firstly, the network characteristics of the B&R land–sea transport network, the MSR shipping network, and China–Europe freight train transport network are compared and analyzed. As shown in Table 1, the average path length of the B&R land–sea transport network is slightly higher than that of the MSR shipping network, and the clustering coefficient, network density, network structure entropy, and average degree are slightly lower. To analyze the reasons, the current development of the China–Europe freight train transport network is weaker than that of the MSR shipping network. As a result, after the B&R land–sea transport network is formed by the MSR shipping network and the China–Europe freight train transport network, the connectivity of the land–sea transport network is somewhat reduced compared with that of the MSR shipping network. On average, nodes in the network need to pass more transit nodes to reach the destination node. The internal connection of the network also has some decline. In addition, since the central node of the China–Europe freight train transport network is often not the central node of the MSR shipping network, the order of the land–sea transport network has been reduced relative to the MSR shipping network, and the trend of centralization has been reduced.

Table 1. Transport network characteristics.

	The B&R Land–Sea Transport Network	The MSR Shipping Network	China–Europe Freight Train Network
Number of nodes	664	594	92
Average path length	2.592	2.521	2.026
Clustering coefficient	0.762	0.765	0.801
Network density	0.036	0.042	0.137
Network structure entropy	3.895	3.917	3.073
Average degree	23.798	24.690	12.435

4.2. Influence of Different Parameters on Network Cascading Failure

The maximum attack frequency and attack threshold (meaning that the giant component size decreases sharply after an attack and the network collapses) of the B&R land–sea transport network and MSR shipping network under the attack strategy based on the maximum point strength are analyzed under different node capacity tolerances (parameter α, from Equation (4)) and local load distribution coefficients (parameter β, from Equation (5)). The results are shown in Tables 2 and 3. Firstly, the maximum attack frequency and attack threshold of the B&R land–sea transport network and the MSR shipping network are compared. It can be seen that in most cases, the attack threshold of the land–sea transportation network is equal to that of the MSR shipping network, and the number of attacks is slightly lower than that of the MSR shipping network.

Table 2. Maximum attack frequency and threshold of the B&R land–sea transport network under maximum point strength attack strategy with different parameters.

		α					
		0	**0.1**	**0.2**	**0.3**	**0.4**	**0.5**
β	0.1	1/1	1/1	1/1	2/1	3/2	4/3
	0.2	1/1	1/1	2/1	2/1	3/2	5/3
	0.3	1/1	2/1	2/1	3/2	4/2	5/3
	0.4	1/1	2/1	2/1	4/2	5/3	8/4
	0.5	1/1	2/1	4/2	5/2	6/3	7/4
	0.6	1/1	3/1	3/2	6/3	8/4	7/4
	0.7	1/1	2/1	4/2	7/3	9/4	9/5
	0.8	1/1	4/1	5/2	8/4	10/5	12/6
	0.9	1/1	2/1	7/3	10/4	10/5	11/6
	1.0	1/1	7/2	9/4	11/5	16/6	20/8
	1.1	1/1	6/2	12/3	13/4	17/6	14/7
	1.2	1/1	10/2	10/3	15/4	8/5	10/6
	1.3	1/1	9/2	9/3	15/4	17/5	16/5
	1.4	1/1	7/1	11/2	6/3	7/4	16/5
	1.5	1/1	10/1	4/2	6/3	9/4	22/4
	1.6	1/1	7/1	6/2	10/3	18/3	18/4
	1.7	1/1	7/1	7/2	12/3	24/3	18/4
	1.8	1/1	6/1	11/2	15/2	15/3	18/3
	1.9	1/1	7/1	16/2	14/2	18/3	21/3
	2.0	1/1	11/1	19/2	16/2	19/3	26/3

In addition, when the node capacity parameter increases, the maximum number of attacks and the attack threshold of the B&R land–sea transport network and the MSR shipping network increase continuously. However, the increase of the capacity parameters means that the node needs to increase the construction scale to enhance the node's ability to face risks, which also means that the node needs to invest more costs. Therefore, the capacity coefficients cannot be increased all the time. In summary, when setting the capacity parameter, 0.2 is more appropriate. At this time, when the load distribution coefficient is 1, the maximum number of attacks on the B&R land–sea transport network is nine times, and

the attack threshold is four times. At the same time, the maximum number of attacks on the MSR network is 13 times, and the attack threshold is 4 times. The B&R land–sea transport network and the MSR network will collapse only after the nodes with the maximum point strength of the four times are removed. When the capacity parameter is set to 0.2, the node input cost is relatively small, and the cascade failure resistance performance of the network is reasonable, so the capacity parameter is set to 0.2.

Table 3. The maximum attack number and threshold of the MSR shipping network under the maximum strength attack strategy with different parameters.

		α					
		0	**0.1**	**0.2**	**0.3**	**0.4**	**0.5**
β	0.1	1/1	1/1	1/1	2/1	3/2	3/2
	0.2	1/1	1/1	2/1	2/1	3/2	5/3
	0.3	1/1	2/1	2/1	3/2	4/2	5/3
	0.4	1/1	2/1	2/1	3/2	7/3	7/4
	0.5	1/1	2/1	2/1	5/2	6/3	6/4
	0.6	1/1	3/1	4/2	6/3	8/4	8/4
	0.7	1/1	2/1	3/2	9/3	11/4	12/5
	0.8	1/1	5/1	10/2	8/4	12/5	16/6
	0.9	1/1	4/2	7/3	13/4	11/5	10/6
	1.0	1/1	7/2	12/4	14/5	19/6	23/8
	1.1	1/1	8/2	12/3	15/4	20/6	19/7
	1.2	1/1	12/2	14/3	15/4	10/5	9/6
	1.3	1/1	12/2	12/3	12/3	6/4	20/5
	1.4	1/1	7/1	11/2	10/3	7/4	16/5
	1.5	1/1	10/1	8/2	9/3	8/4	17/4
	1.6	1/1	8/1	5/2	7/3	22/3	19/4
	1.7	1/1	8/1	8/2	9/2	22/3	19/4
	1.8	1/1	10/1	11/2	19/2	15/3	23/3
	1.9	1/1	8/1	15/2	17/2	18/3	21/3
	2.0	1/1	11/1	17/2	19/2	22/3	29/3

In addition, the influence of local load parameters β on the failure resistance of the network cascade is analyzed. It can be seen that when α = 0.1~0.5 and β = 1, the attack threshold of B&R land–sea transport network and MSR shipping network is the largest. This shows that when the local load factor is 1, the cascade failure resistance of the network is better.

In summary, α = 0.2 and β = 1 are more appropriate. Therefore, in the following sections, the changes in the cascade failure resistance of the B&R land–sea transport network and the MSR network is analyzed for $\alpha = 0.2$ and $\beta = 1$.

4.3. Evaluation of Network Robustness under Different Attack Strategies

To analyze the change in network cascade failure resistance under different attack strategies, parameters $\alpha = 0.2$ and $\beta = 1$ are set in Equation (4). Based on the random attack strategy, maximum point strength attack strategy, maximum degree attack strategy, and maximum betweenness attack strategy, we simulated cascade failure of the B&R land–sea transport network (in which random attack was simulated 10 times). The cascade failure simulation of the MSR shipping network is carried out for comparison.

This can be seen in Figure 4a. First, over the course of 10 random attacks, each attack threshold exceeds 32. This indicates that the B&R land–sea transport network has better resistance to network cascade failure under random attack. In addition, the damage resistance under deliberate attack is analyzed, as shown in Figure 4b–d. It can be seen that under the attack strategy of maximum point strength, maximum degree, and maximum betweenness, the node retention rate of the land–sea transportation network decreases very fast. Therefore, under the deliberate attack strategies, the land–sea transport network is extremely vulnerable to cascading failure.

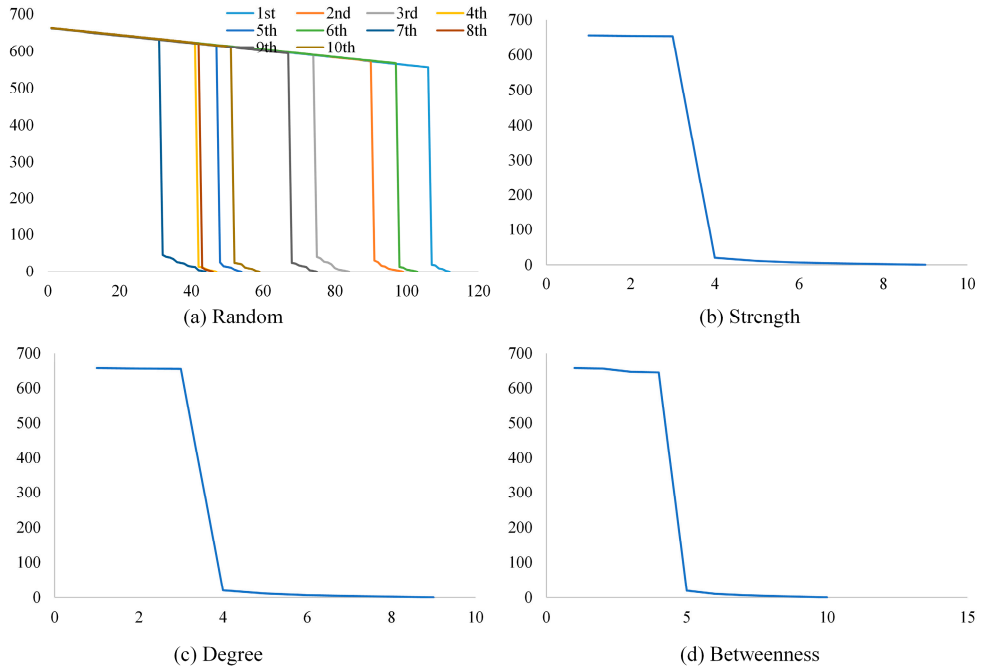


Figure 4. Node retention rates of the B&R land–sea transport network under different attack strategies.

Then, compare the B&R land–sea transport network with the MSR shipping network. The results are shown in Figures 4 and 5, from the results of random attacks, the variation amplitude of maximum attack times and attack threshold of the B&R land–sea transportation network is greater than that of the MSR shipping network. The reason may be that, on the one hand, there are more nodes in the B&R land–sea transport network than the MSR shipping network, and random attack strategy may attack many nodes with less strength. On the other hand, the strength of some nodes in the B&R land–sea transport network is greater than that of the MSR shipping network, and random attack strategy may also attack these nodes with greater strength.

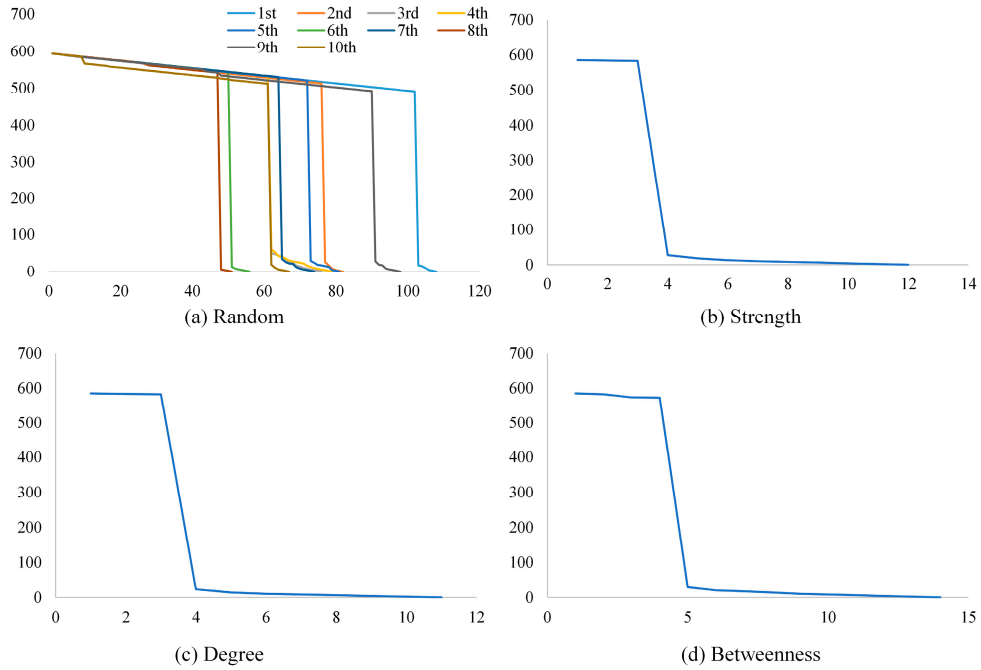


Figure 5. Node retention rates of the MSR network under different attack strategies.

In addition, from the point of view of deliberate attack, the attack threshold of the B&R land–sea transportation network is the same as that of the MSR shipping network. The maximum number of attacks is slightly less than that of the MSR shipping network. By analyzing the reasons, it is believed that the current development of China–Europe freight train transportation lags behind that of the MSR shipping, and the MSR shipping freight flow is dominant in the network, so the land transportation node cannot withstand the freight volume from the shipping, and the cascading failure robustness of the land–sea transportation network has not been improved.

Next, the changes in network efficiency and giant component size are analyzed. As shown in Figures 6–9, the changes in network efficiency and giant component size are consistent with the results of node retention. Under the random attack strategy, the B&R network efficiency changes slightly. After 31 iterations in 10 simulations, the efficiency of the network is maintained at 70.2–71.2%. The giant component size of the network is maintained at 95.0–95.3%. After 32 iterations, the efficiency of the network and the giant component size begin to decline significantly.

However, under the attack strategy of maximum point strength, maximum degree, and maximum betweenness, the efficiency and giant component size of the land–sea transport network rapidly decrease. Under the attack strategies of maximum point strength and maximum degree, the network efficiency of land–sea transportation network decreases to 0.04% and 0.04%, respectively, in the fourth iteration, and the giant component size decreases to 1.36% and 1.36%, respectively. Under the attack strategy of maximum betweenness, the network efficiency decreases to 0.04% and the giant component size decreases to 1.36% in the fifth iteration.

In addition, the B&R land–sea transportation network is compared with the MSR shipping network. The results of network efficiency and giant component size are consistent with the results of node retention.

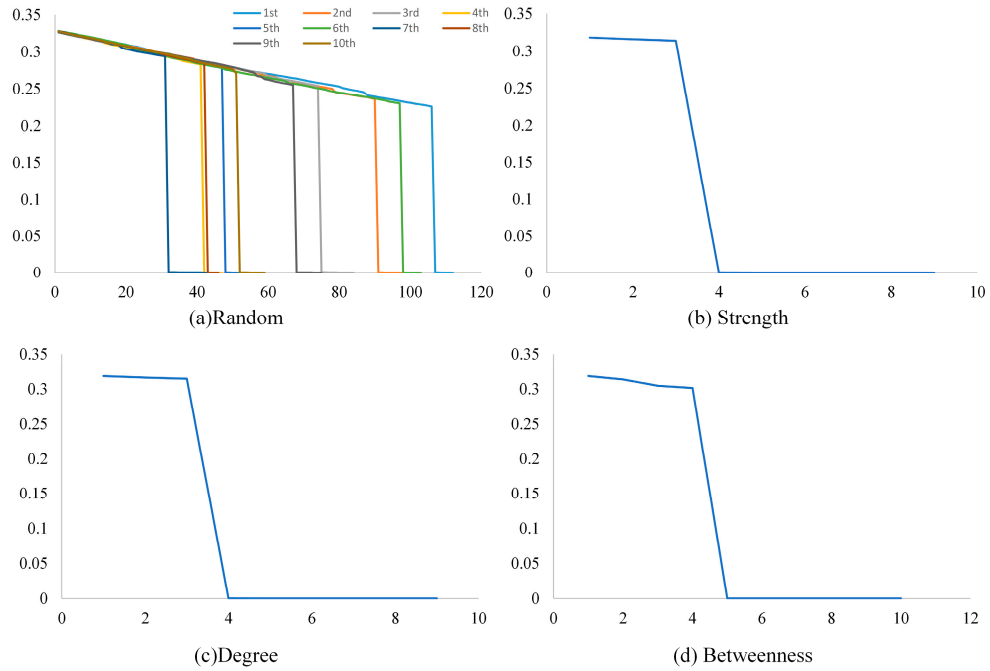


Figure 6. The B&R land–sea transportation network efficiency under different attack strategies.

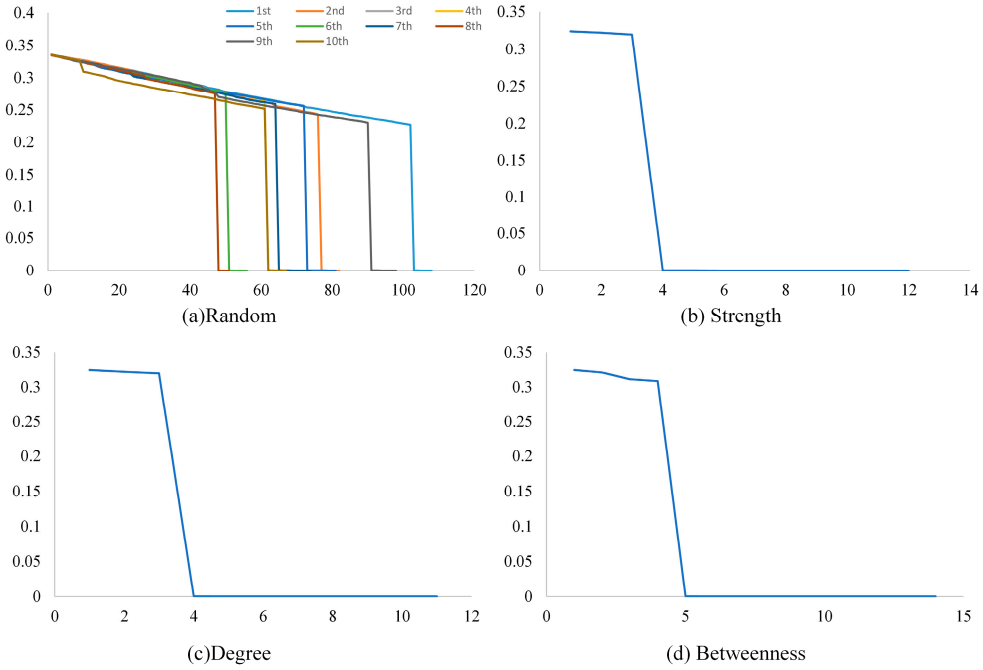


Figure 7. MSR network efficiency under different attack strategies.

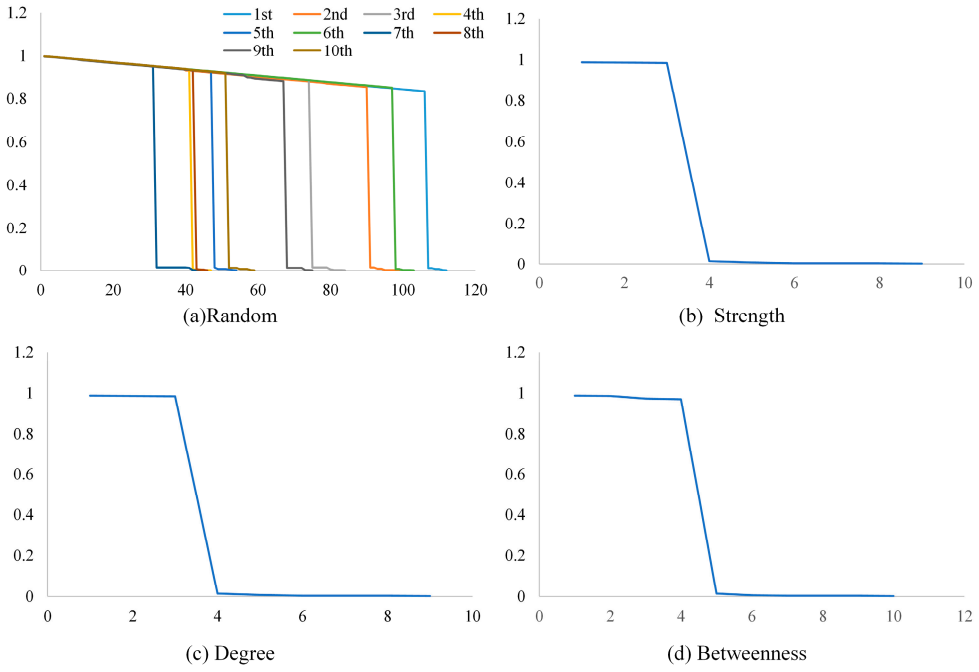


Figure 8. Giant component size of the B&R land–sea transportation network under different attack strategies.

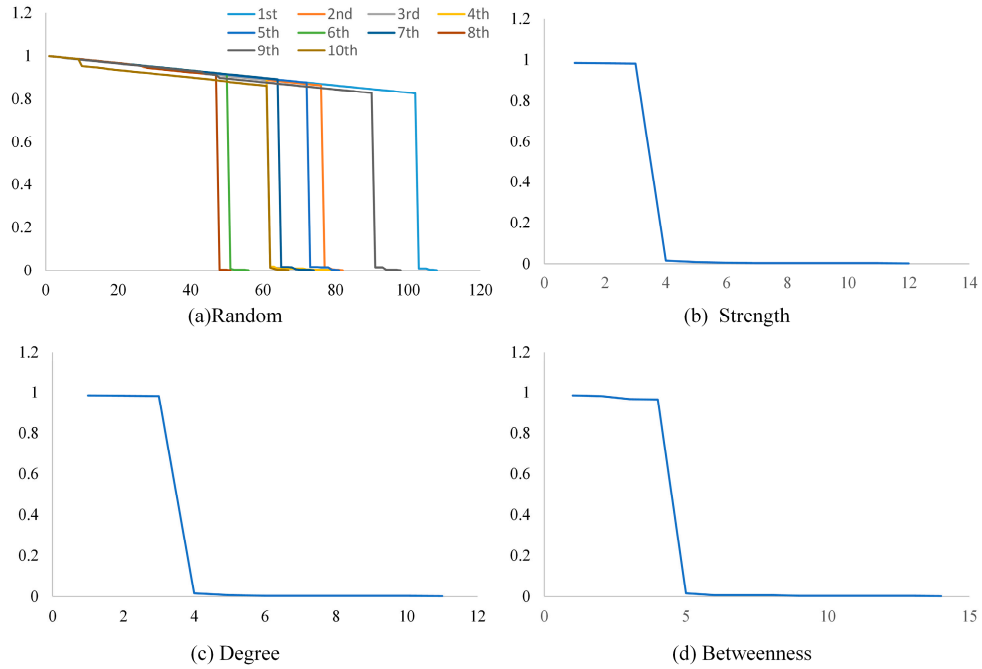


Figure 9. Giant component size of the MSR network under different attack strategies.

4.4. Deliberate Attack Analysis

In addition, the order of attacked nodes and the changes in the efficiency of the networks E (calculated by Equation (7)) under a deliberate attack strategy are analyzed. The results are shown in Table 4, under the maximum point strength attack strategy, the attacked nodes in the land–sea transport network and the MSR shipping network are Shanghai, Shenzhen, and Singapore, and the network crashes. Under the maximum degree attack strategy, the attacked nodes in the land–sea transport network and the MSR shipping network are Shanghai, Singapore, and Ningbo, and the network crashes. Under the maximum betweenness attack strategy, the attacked nodes in the land–sea transport network are Shanghai, Hamburg, Guangzhou, and Busan, and the network crashes. The MSR shipping network is attacked in the order of Shanghai, Busan, Guangzhou, and Hamburg, and the network crashed.

Table 4. The order of attacked nodes and network efficiency under deliberate attack strategy.

Attack Order	The B&R Land–Sea Transport Network			The MSR Shipping Network		
	Maximum Point Strength Attack	**Max Degree Attack**	**Maximum betweenness Number Attack**	**Maximum Point Strength Attack**	**Max Value Attack**	**Maximum Interface Attack**
1	Shanghai (0.318)	Shanghai (0.318)	Shanghai (0.318)	Shanghai (0.324)	Shanghai (0.324)	Shanghai (0.324)
2	Shenzhen (0.316)	Singapore (0.316)	Hamburg (0.314)	Shenzhen (0.322)	Singapore (0.321)	Pusan (0.321)
3	Singapore (0.314)	Ningbo (0.315)	Guangzhou (0.305)	Singapore (0.32)	Ningbo (0.319)	Guangzhou (0.311)
4	Ningbo (1.73×10^{-4})	Shenzhen (1.73×10^{-4})	Pusan (0.302)	Ningbo (2.29×10^{-4})	Pusan (1.94×10^{-4})	Singapore (0.309)
5	Oulu (5.91×10^{-5})	Oulu (5.91×10^{-5})	Singapore (1.51×10^{-4})	Oulu (8.66×10^{-5})	Oulu (5.11×10^{-5})	Hamburg (2.15×10^{-4})
6	Abadan (1.36×10^{-5})	Abadan (1.36×10^{-5})	Oulu (3.63×10^{-5})	Abadan (2.98×10^{-5})	Kumamoto (2.27×10^{-5})	Oulu (7.24×10^{-5})

Table 4. *Cont.*

Attack Order	The B&R Land–Sea Transport Network			The MSR Shipping Network		
	Maximum Point Strength Attack	**Max Degree Attack**	**Maximum betweenness Number Attack**	**Maximum Point Strength Attack**	**Max Value Attack**	**Maximum Interface Attack**
7	Bengbu (9.09×10^{-6})	Bengbu (9.09×10^{-6})	Imari (1.36×10^{-5})	Longtan (2.27×10^{-5})	Bengbu (1.7×10^{-5})	Longtan (6.53×10^{-5})
8	Goa (4.54×10^{-6})	Goa (4.54×10^{-6})	Yangzhou (9.09×10^{-6})	Chongqing (1.99×10^{-5})	Chongqing (1.42×10^{-5})	Ras al khaimah (5.11×10^{-5})
9	Port d'ehoala (0)	Port d'ehoala (0)	Goa (4.54×10^{-6})	Jingzhou (1.7×10^{-5})	Goa (8.52×10^{-6})	Imari (2.27×10^{-5})
10			Tulear (0)	Bengbu (1.14×10^{-5})	Jingzhou (5.68×10^{-6})	Yangzhou (1.7×10^{-5})
11				Goa (5.68×10^{-6})	Port d'ehoala (0)	Wuhan (1.42×10^{-5})
12				Port d'ehoala (0)		Yibin (1.14×10^{-5})
13						Goa (5.68×10^{-6})
14						Tulear (0)

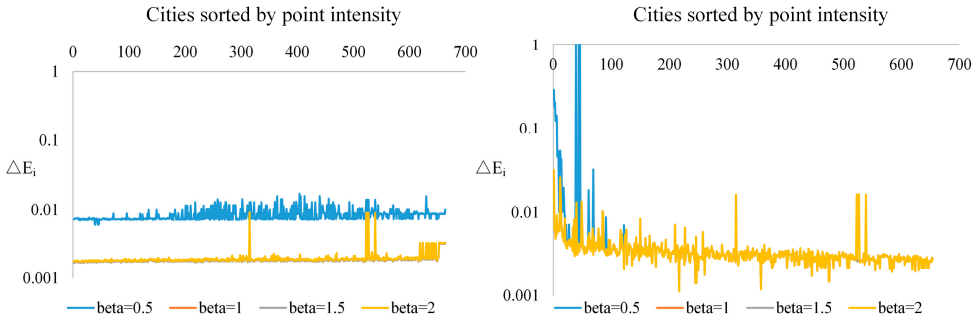
The results show that the number of attacked nodes in the B&R land–sea transport network is the same as that in the MSR shipping network under maximum point strength and maximum degree attack strategy. Under the maximum betweenness attack strategy, the number of attacked nodes before the network crash is the same, and the order of nodes changes. In general, under deliberate attack, the order of attacked nodes in the B&R land–sea transport network and the MSR shipping network basically do not change before reaching the attack threshold. This shows that since the current development of China–Europe freight trains lags far behind that of the MSR, the hub nodes of the B&R land–sea transport network are basically the same as those of the MSR shipping network, resulting in little change in the order of nodes attacked under deliberate attack.

4.5. Analysis of Node Vulnerability and Criticality

Considering cascade failure propagation, the change in the node or network efficiency index is analyzed from the perspective of node vulnerability and node criticality. The results are shown in Figures 10 and 11. Firstly, in the B&R land–sea transport network, node vulnerability is negatively correlated with node strength, and nodes with greater strength are less vulnerable. When the local load distribution coefficient β is 0.5, the node vulnerability is mostly approximately 7×10^{-3}. When β is 1, 1.5, or 2, the distributions of port node vulnerability are basically the same, and most of the node vulnerabilities are approximately 1.7×10^{-3}. This indicates that the vulnerability of nodes is greater at small times than when the local load distribution coefficient β is large, and the efficiency of the node is relatively easily affected by other initially attacked nodes. When the local load distribution coefficient exceeds 1, the node vulnerability is not affected by the distribution load distribution coefficient. This also corresponds to the research results in Section 4.2; when the local load distribution coefficient is small, the network is more prone to collapse. In addition, the efficiency of small nodes is more susceptible to the impact of other nodes that are initially attacked.

In addition, as shown in Figure 10b, first, there is a positive correlation between node criticality and point strength. When β is 0.5, the node criticality of cities with high point strength is greater. The node criticality of the top 13 cities with high point strengths is greater than 5×10^{-2}, while that of the following ports is mostly less than 2×10^{-2}. When β is 1, 1.5 or 2, the distributions of city node criticality are basically the same. The criticality

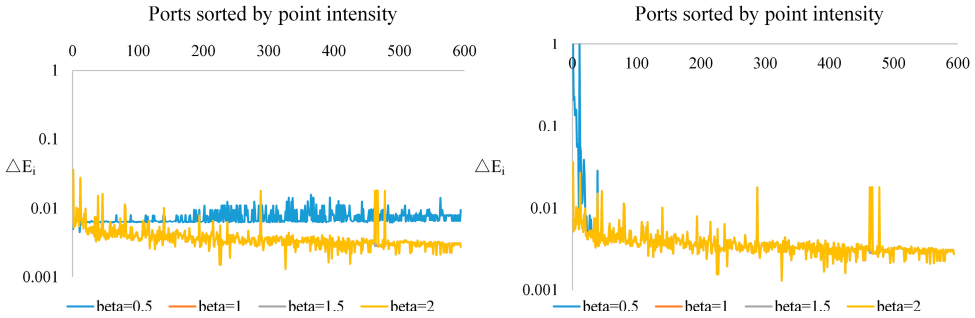
of Shanghai is 3.2×10^{-2}, and those of the other nodes are all below 2×10^{-2}. Moreover, the value of β has no effect on the node criticality in cities with point strength rankings lower than 28. This shows that for cities with larger point strengths, the value of β has some influence on node criticality. When the value of β is small, the failure of cities with greater point strength will lead to a reduction in network efficiency, while the failure of small cities has little influence on the efficiency of the network. When the value of β exceeds 1, the network shows good robustness after one attack iteration, so the criticality of any node is low.



(a) Dynamic vulnerability (b) Dynamic criticality

Note: The cities on the abscissa are ordered by point intensity

Figure 10. Dynamic vulnerability and criticality of the B&R land–sea transport network nodes, when $\alpha = 0.2$.



(a) Dynamic vulnerability (b) Dynamic criticality

Note: The ports on the abscissa are ordered by point intensity

Figure 11. Dynamic vulnerability and criticality of the MSR shipping network ports, when $\alpha = 0.2$.

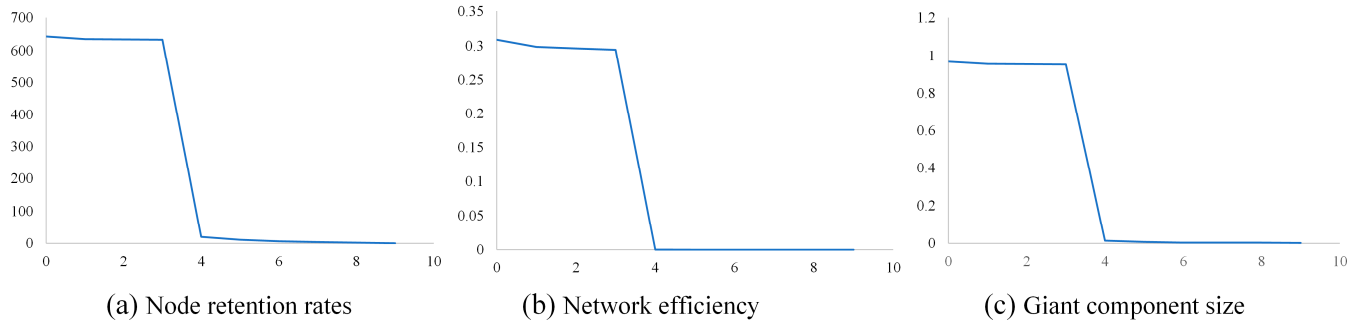
In addition, the B&R land–sea transport network is compared with the MSR shipping network. When β is 0.5, the node vulnerability and node criticality of the land–sea transport network are higher than that of the MSR shipping network. When β is 1, 1.5, or 2, the node vulnerability and node criticality of the land–sea transport network are lower than that of the MSR shipping network. By analyzing the reasons, it is concluded that when β is small, the land–sea transport network generates more cargo flow, and when the cargo flow of attacked nodes is evenly distributed, the efficiency of nodes and network will be more susceptible to the impact of the initial attacked nodes. When β is large, the cargo traffic of the attacked node is more easily distributed by the node with greater strength, and the node strength of the land–sea transport network is greater than that of the MSR network, so the efficiency of the node and network is not easily affected by the initial attacked node.

4.6. Analysis of Network Robustness under Emergencies

4.6.1. Network Robustness Analysis under the Russia–Ukraine Conflict

Then the changes of land–sea network robustness under the Russia–Ukraine conflict are analyzed. Based on the analysis of the Russia–Ukraine conflict from the perspective of

network, we believe that in this case, the relevant nodes of Russia and Ukraine are attacked, and the traffic of these nodes is transferred to the adjacent nodes, and the cascade failure simulation is carried out. Therefore, a new network is formed, and the maximum strength attack strategy is carried out on the new network, and the cascade failure simulation is carried out again. The obtained network results are shown in Figure 12.



(a) Node retention rates (b) Network efficiency (c) Giant component size

Figure 12. Changes in the cascade failure robustness of networks under the Russia–Ukraine conflict.

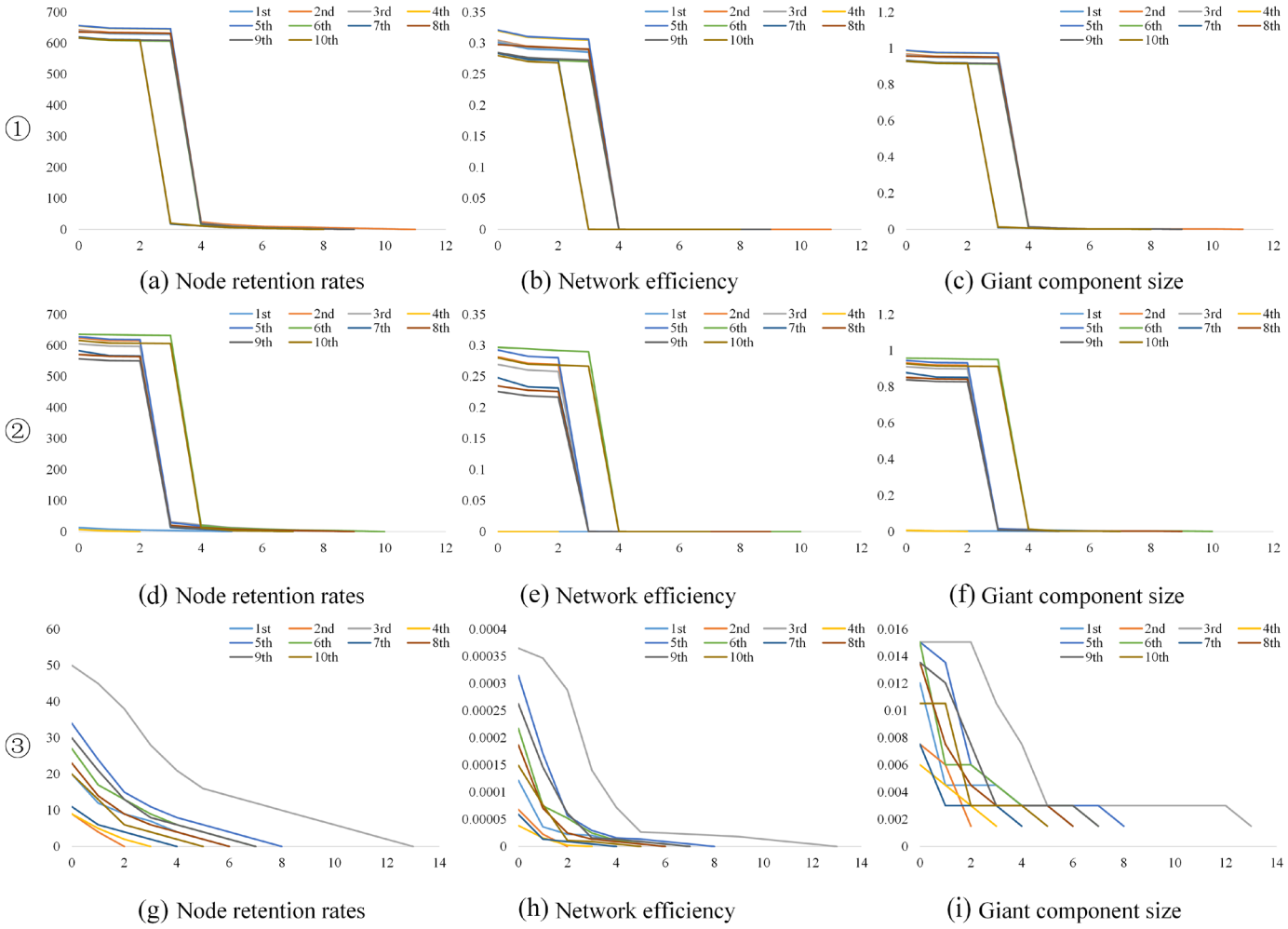
It can be seen that under the Russia–Ukraine conflict, the node retention rate, efficiency, and giant component size of the network drop to 96.8%, 73.9%, and 96.8%, respectively. The cascaded failure robustness analysis of the affected network shows that the network still crashes under the fourth iteration of the attack. Therefore, the cascade failure robustness of the land–sea transport network is currently less affected by the Russia–Ukraine conflict. However, with the rapid development of China–Europe freight trains, the proportion of land transport in the B&R land–sea transport network will continue to increase. Therefore, in the future, it is necessary to monitor the geopolitical risk factors along the China–Europe railway line and recalculate the cascade failure robustness according to the network development. Policymakers should analyze the circumstances in which these risk factors will cause significant damage to the network and develop appropriate preventive measures.

4.6.2. Network Robustness Analysis under the Red Sea Crisis

In addition, the changes of land–sea network robustness under the Red Sea crisis are analyzed. According to the analysis of the Red Sea crisis from the perspective of network, the Asia–Europe shipping network could be attacked by 5–20% of the transport links in this situation. Three scenarios are designed to transform the attacks of transport links into attacks of nodes. ① Some nodes are removed from ports in Asia or Europe, and the strength value of nodes removed accounts for 5%. ② The strength value of the nodes removed accounts for 10%. ③ The strength value of the nodes removed accounted for 20% (due to the randomness of removing some nodes, the Asia–Europe port removed nodes for 10 times of simulation). After removing the nodes, the traffic of the nodes is distributed to the neighbor nodes, and the cascade failure simulation is carried out. A new network is obtained, and then the maximum strength attack strategy is carried out on the new network, and the cascade failure simulation is performed again. The network results obtained are shown in Figure 13.

It can be seen that in the first scenario, the node retention rates, efficiency, and giant component size of the network drop to 92.9–98.9%, 67.0–76.8%, and 92.9–98.9%, respectively. The network still crashes under the fourth iteration of the attack. This indicates that the cascade failure robustness of the network was less affected in the scenario of an attack in which the Red Sea crisis caused 5% of the Asia–Europe maritime network transport links. In the second scenario, the network has eight simulations with node retention rates of more than 83.9% and two simulations with node retention rates of less than 2.0%. Six of the eight simulations with high network node retention rates have network attack thresholds of 3, and two have network attack thresholds of 4. It shows that in the second scenario, there is a 20% chance that the network will crash directly, a 60% chance that the network cascade failure robustness will be significantly reduced, and only a 20% chance that the network

cascade failure robustness will be little affected. In the third case, the retention rates of the network decrease to 1.4–7.5% after 10 simulations. This shows that in the third case, the network will crash directly.



Note: ① indicates that 5% of the transport links in the Asia-Europe shipping network are attacked as a result of the Red Sea crisis, ② indicates that 10% are attacked, and ③ indicates that 20% are attacked.

Figure 13. Changes in network cascade failure robustness under the Red Sea crisis.

On the whole, if the Red Sea crisis affects 5% of Asia–Europe shipping links, the cascading failure robustness of the land–sea transport network will be less affected. If 10% of Asia–Europe maritime links are affected, the cascading failure robustness of the network is more likely to be significantly affected, and the direct collapse of the network is less likely. If 20% of Asia–Europe maritime links are affected, the network will collapse directly. Therefore, it is important for policy makers to analyze the impact of the Red Sea crisis and take timely measures.

4.7. Network Cascade Failure Robustness Analysis Considering More Factors

In addition, it should be recognized that there are many other factors that affect the cascading failure robustness of the B&R land–sea transport network. For example, the power of the host country of the city node, inter-state cooperation, and road quality may affect the cascade failure robustness of the network. Therefore, more elements should be added to the cascade failure model to analyze the influence of these factors on the cascade failure robustness of the network. The selected factors include the national power factor, inter-national cooperation factor, and road quality factor. It is believed that the

greater the national power and the more cooperation between countries, the better the road quality, and the less vulnerable the node cities in the country are to attack. The power of a country can be represented by available GDP, the cooperation factors between countries can be represented by the foreign trade volume of a country, and the road quality can be represented by the liner shipping connectivity index (*LSCI*) released by UNCTAD.

Therefore, the Equation for the possibility P_i of a node being attacked can be established as follows.

$$P_i = \frac{s_i}{GDP_i \cdot T_i \cdot LSCI_i} \tag{11}$$

where s_i represents the point strength of node i, GDP_i represents the GDP of the country where node i is located (unit: trillion US dollars, if $GDP_i < 0.1$, GDP_i is 0.1), T_i represents the foreign trade volume of the country where node i is located (unit: trillion US dollars, if $T_i < 0.1$, T_i is 0.1), $LSCI_i$ represents the *LSCI* of the country where node i is located (unit: hundred, if $LSCI_i < 0.1$, $LSCI_i$ is 0.1).

Node cities are attacked in order of P_i from largest to smallest, and the remaining steps are the same as ②–④ in Section 3.1. Among them, the national GDP data and the international foreign trade volume data are from the World Bank, and the data are taken from 2021.

When analyzing the influence of national power factors on network robustness, only GDP_i value is taken in Equation (10). Similarly, when the influence of national cooperation factors or road quality factors on network robustness is analyzed, only the value of T_i or only the value of $LSCI_i$ is taken from Equation (10). The results obtained are shown in Table 5.

Table 5. The order of attacked nodes and network efficiency under other attack strategies.

	Attack Strategy under the Influence of National Power	Attack Strategy under the Influence of National Cooperation	Attack Strategy under the Influence of Road Quality
1	Clombo (0.328)	Clombo (0.328)	Minsk (0.328)
2	Singapore (0.325)	Piraeus (0.326)	Alma-Ata (0.327)
3	Klang (0.323)	Port said (0.325)	Ulan Bator (0.326)
4	Minsk (0.322)	Minsk (0.324)	Pointe des galets (0.324)
5	Piraeus (0.321)	Tangier (0.322)	Singapore (0.322)
6	Salalah (0.319)	Singapore (0.32)	Pusan (0.319)
7	Beirut (0.318)	Klang (0.318)	Piraeus (2.07×10^{-4})
8	Tangier (0.317)	Alma−Ata (1.82×10^{-4})	Oulu (9.31×10^{-5})
9	Malta (0.315)	Oulu (6.74×10^{-5})	Lobito (9.09×10^{-5})
10	Tanjung pelepas (9.09×10^{-6})	Lobito (6.51×10^{-5})	Abadan (4.54×10^{-5})
11	Port d'ehoala (4.54×10^{-6})	Abadan (1.97×10^{-5})	Port d'ehoala (4.09×10^{-5})
12	Goa (0)	Panjang (1.51×10^{-5})	Panjang (3.63×10^{-5})
13		Kolkata (1.36×10^{-5})	Ahus (3.18×10^{-5})
14		Port d'ehoala (9.09×10^{-6})	Bengkulu (2.73×10^{-5})
15		Ahus (4.54×10^{-6})	Kumamoto (4.54×10^{-6})
16		Bengkulu (0)	Yangzhou (0)

It can be seen that under the influence of factors such as national power, national cooperation, and road quality, the attack threshold of the network becomes 10, 8, and 7 respectively. The results show that under the influence of these factors, the robustness of the B&R land–sea transport network will be improved to varying degrees. Among them, the national power factor has the greatest impact on the network robustness, followed by the national cooperation, and the road quality is low. In addition, under the influence of these factors, the cities attacked before the network crash are mainly Southeast Asian cities. Under the attack strategy influenced by national power, the large city attacked is Singapore. Under the attack strategy of national cooperation, the large city under attack is Singapore. Under the attack strategy under the effect of road quality, the large ports attacked are Singapore and Pusan. Looking back at Table 4, the large cities attacked

under the maximum point strength attack strategy are Shanghai, Shenzhen, Singapore, and Ningbo. This shows that due to China's strong national power and road quality and the country's close cooperation with foreign countries, China's large cities are not easy to attack. Therefore, China's large ports are not attacked, which plays a positive role in improving the cascade failure robustness of the B&R land–sea transport network.

4.8. Comparative Analysis

In addition, in order to analyze the validity of this study, the study in this paper is compared with existing relevant studies. Relevant representative studies are selected as follows: Xu et al. [28], Xu et al. [33], and Jiang et al. [34]. The comparison is shown in Table 6.

Table 6. The characteristics of this study and other studies.

	Methods	Problems	Results
Xu et al. [28]	A novel cascading model, which incorporates the realistic factor of liner shipping service routes' behavior of port rotation adjustments under port failures	The static and dynamic vulnerability of global container shipping network	The global container shipping network under cascading failures is significantly more vulnerable than its static structure. Choosing alternative ports increases the GLSN vulnerability to cascading failures.
Xu et al. [33]	A Motter-Lai overload model	The vulnerability, reliability, potential risks, and possible impacts of the global container shipping network	The regional characteristics of port failure patterns can be roughly divided into three regions: Northeast Asia, Southeast Asia, and EU–North America. Northeast Asia patterns typically encompass the ports of Shanghai and Kao-Hsiung.
Jiang et al. [34]	An enhanced cascading failure model grounded in a nonlinear capacity framework	The static and dynamic vulnerability of the Maritime Silk Road shipping network	The network's static structure is exceedingly susceptible to disruptions at ports with high connectivity, whereas in the context of cascading failures, the greatest vulnerability lies in ports with substantial load.
This study	A cascade failure model considering the impact of emergencies	The cascading failure robustness of the B&R land–sea transport network under emergencies	Russia–Ukraine conflict has little effect on the cascade failure robustness of land–sea transport network. The Red Sea crisis may have a significant impact on the robustness of the cascading failures of land–sea transport network.

As can be seen from Table 6, the results of various studies are different.

(1) Xu et al. [28], Xu et al. [33], and Jiang et al. [34] all improved the traditional network cascade failure model. In this paper, a cascade failure model considering emergency events is presented. In general, each study has its own characteristics in terms of research methods.

(2) Xu et al. [28], Xu et al. [33], and Jiang et al. [34] all studied the cascading failure vulnerability of shipping networks. This paper analyzes the cascading failure robustness of the B&R land–sea transport network, with some differences in research perspectives.

(3) Xu et al. [28], Xu et al. [33], and Jiang et al. [34] all studied the cascade failure vulnerability of shipping networks through the change of node parameters. This paper analyzes the influence of emergencies on the robustness of network cascade failure. This paper focuses more on the combination of network and actual events, which shows some advantages in this aspect.

4.9. Discussion

Based on the previous analysis of the cascade failure results of the B&R land–sea transport network, five suggestions on improving the cascade failure robustness of the B&R land–sea transport network are discussed.

(1) Reasonable distribution of cargo flow in the attacked node. According to the previous analysis, when the local load distribution coefficient is too large or too small, the collapse of the B&R land–sea transport network will accelerate. When the local load distribution coefficient is 1, the cargo traffic of the attacked node allocated to the neighbor should be proportional to the point strength of the neighbor, which can reduce the impact of node failure on the cascade failure robustness of the network.

(2) Promote the development of China–Europe freight trains and balance the Eurasian land–sea transport pattern. According to the analysis, the cascade failure robustness of the B&R land–sea transport network is not better than that of the MSR shipping network. The reason is that the China–Europe freight trains lagged behind the development of the MSR, and the land transport nodes could not bear the freight volume from sea. Therefore, China–Europe freight trains should be further promoted, such as the construction of the southern corridor (China–Turkey—Central and Eastern Europe), and the coverage of China–Europe freight trains should be increased.

(3) To undertake part of the B&R land–sea transport network cargo flow through the Arctic routes. It is feasible to improve the cascade failure robustness of the B&R land–sea transport network, expand port terminals and storage yards, expand the scale of container freight stations in inland cities, and enhance the container handling efficiency of ports and inland node cities, so as to improve the capacity parameters of nodes. However, this strategy may mean that more investment is placed on preventing nodes from being attacked, and there is no way to improve the transportation efficiency of areas along the B&R, and the benefits of this strategy are poor. It is believed that the Arctic routes can be built to bear part of the cargo flow of the B&R land–sea transportation network. On the one hand, by reducing the cargo flow of the B&R land–sea transport network, the surplus between node capacity and node load can be increased, so that each node can better bear the cargo flow distribution caused by the failure of neighboring nodes. On the other hand, by forming the transport pattern of the traditional Suez Canal route, Arctic routes, and China–Europe freight train, the transport efficiency of the B&R can be improved.

(4) Emergencies such as the Red Sea crisis may have a significant impact on the cascading failure robustness of the land–sea transport network, and even lead to network collapse. After the occurrence of emergencies, decision-makers should conduct quantitative analysis of the impact of emergencies in time and make some plans to reduce the impact of emergencies on the land–sea transport network.

(5) Strengthening national cooperation. According to the previous analysis, both national cooperation and road quality factors can significantly improve the cascade failure robustness of land–sea transport networks. Countries along the route should make overall plans, strengthen port construction along the MSR, and promote the construction of more routes for China–Europe express trains. In addition, countries with significant international power should exert their influence and call on countries along the routes to cooperate to enhance the robustness of the network.

5. Conclusions

In order to ensure the security of the B&R land–sea transport network, this study established a network cascade failure model and quantitatively analyzed the robustness index of the B&R land–sea transport under cascade failure from the perspectives of random attack, deliberate attack, and real emergencies. The specific advantages and contributions of this paper are summarized as follows.

(1) This paper constructs the B&R land–sea transport network, analyzes the cascade failure robustness of Eurasian transport network from the comprehensive perspective of

land–sea transport, and provides a new perspective for the study of the cascade failure problem of the Eurasian transport system.

(2) Taking real emergencies (Russia–Ukraine crisis and Red Sea crisis) as examples, this paper analyzes the cascade failure robustness of the B&R land–sea transport network, providing a new research framework for the safety analysis of the Eurasian transport system under emergencies.

(3) This paper can provide a reference for the cascade failure robustness analysis of other networks under emergencies. For example, the air transport network will also be affected by emergencies (such as COVID-19 and geopolitical factors). Some airports or routes will be closed, and their passenger or cargo traffic will be allocated to adjacent airport routes, which also has the problem of cascade failure robustness. This research can provide reference for the cascade failure analysis of these transport networks.

However, there are still some problems in this paper that need to be improved upon in the future: (1) This paper designs the attack strategy with maximum strength, maximum degree, and maximum betweenness, while the real attack strategy may be related to the attributes of nodes (such as the political stability of the country where the cities are located). In the future, the robustness of the B&R land–sea transport network can be analyzed by combining the attributes of nodes and other factors. (2) The external emergencies designed in this paper are not comprehensive enough to affect the transport network, so we should analyze the external emergencies more deeply in the future.

Author Contributions: Conceptualization, C.D. and Z.W.; methodology, C.D.; software, C.D.; validation, C.D.; formal analysis, C.D.; investigation, C.D. and Z.W.; resources, C.D. and Z.W.; data curation, C.D.; writing—original draft preparation, C.D. and S.X.; visualization, C.D. and S.X.; supervision, C.D.; project administration, C.D.; writing—review and editing, C.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Talent Introduction Research Fund, China under Zhejiang Ocean University [JX6311180823].

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. China-Europe Freight Train Services See Solid Growth in First 11 Months. Available online: https://english.www.gov.cn/news/202312/06/content_WS656fe5f6c6d0868f4e8e1ee7.html (accessed on 6 December 2023).
2. Xu, M.; Deng, W.; Zhu, Y.; Lu, L. Assessing and improving the structural robustness of global liner shipping system: A motif-based network science approach. *Reliab. Eng. Syst. Saf.* **2023**, *240*, 109576. [CrossRef]
3. Peng, P.; Cheng, S.; Chen, J.; Liao, M.; Wu, L.; Liu, X.; Lu, F. A fine-grained perspective on the robustness of global cargo ship transportation networks. *J. Geogr. Sci.* **2018**, *28*, 881–889. [CrossRef]
4. Wang, N.; Wu, N.; Dong, L.L.; Yan, H.K.; Wu, D. A study of the temporal robustness of the growing global container-shipping network. *Sci. Rep.* **2016**, *6*, 34217. [CrossRef] [PubMed]
5. Achurra-Gonzalez, P.E.; Angeloudis, P.; Goldbeck, N.; Graham, D.J.; Zavitsas, K.; Stettler, M.E. Evaluation of port disruption impacts in the global liner shipping network. *J. Shipp. Trade* **2019**, *4*, 3. [CrossRef]
6. Ducruet, C. The polarization of global container flows by interoceanic canals: Geographic coverage and network vulnerability. *Marit. Policy Manag.* **2016**, *43*, 242–260. [CrossRef]
7. Xie, T.; Zhang, Q.; Xiong, X. Robustness Analysis of Exponential Synchronization in Complex Dynamic Networks with Time-Varying Delays and Random Disturbances. *Symmetry* **2023**, *15*, 1510. [CrossRef]
8. Zarghami, S.A.; Dumrak, J. Unearthing vulnerability of supply provision in logistics networks to the black swan events: Applications of entropy theory and network analysis. *Reliab. Eng. Syst. Saf.* **2021**, *215*, 107798. [CrossRef]
9. Hu, S.; Li, G. TMSE: A topology modification strategy to enhance the robustness of scale-free wireless sensor networks. *Comput. Commun.* **2020**, *157*, 53–63. [CrossRef]
10. Li, M.; Wang, H.; Wang, H. Resilience assessment and optimization for urban rail transit networks: A case study of Beijing Subway Network. *IEEE Access* **2019**, *7*, 71221–71234. [CrossRef]
11. Zhang, J.; Zhou, Y.; Wang, S.; Min, Q. Critical station identification and robustness analysis of urban rail transit networks based on comprehensive vote-rank algorithm. *Chaos Solitons Fractals* **2024**, *178*, 114379. [CrossRef]
12. Cats, O.; Krishnakumari, P. Metropolitan rail network robustness. *Phys. A* **2020**, *549*, 124317. [CrossRef]

13. Pagani, A.; Mosquera, G.; Alturki, A.; Johnson, S.; Jarvis, S.; Wilson, A.; Guo, W.; Varga, L. Resilience or robustness: Identifying topological vulnerabilities in rail networks. *R. Soc. Open Sci.* **2019**, *6*, 181301. [CrossRef] [PubMed]
14. Xie, Y. Robustness of maritime network along the Maritime Silk Road based on trajectory data. *IOP Conf. Ser. Earth. Environ. Sci.* **2019**, *310*, 022034. [CrossRef]
15. Mou, N.; Sun, S.; Yang, T.; Wang, Z.; Zheng, Y.; Chen, J.; Zhang, L. Assessment of the resilience of a complex network for crude oil transportation on the Maritime Silk Road. *IEEE Access* **2020**, *8*, 181311–181325. [CrossRef]
16. Yang, Y.; Liu, W. Resilience analysis of maritime silk road shipping network structure under disruption simulation. *J. Mar. Sci. Eng.* **2022**, *10*, 617. [CrossRef]
17. Lyu, M.; Shuai, B.; Zhang, Q.; Li, L. Ripple effect in China–Europe Railway transport network: Ripple failure risk propagation and influence. *Phys. A* **2023**, *620*, 128739. [CrossRef]
18. Bak, T. Mechanisms of Avalanche Dynamics in£. *Phys. Rev. Lett.* **1987**, *59*, 381. [CrossRef] [PubMed]
19. Motter, A.E.; Lai, Y.C. Cascade-based attacks on complex networks. *Phys. Rev. E* **2002**, *66*, 065102. [CrossRef] [PubMed]
20. Moreno, Y.; Gomez, J.B.; Pacheco, A.F. Instability of scale-free networks under node-breaking avalanches. *Europhys. Lett.* **2002**, *58*, 630. [CrossRef]
21. Wang, W.X.; Chen, G. Universal robustness characteristic of weighted networks against cascading failure. *Phys. Rev. E* **2008**, *77*, 026101. [CrossRef]
22. Qian, Y.; Wang, B.; Xue, Y.; Zeng, J.; Wang, N. A simulation of the cascading failure of a complex network model by considering the characteristics of road traffic conditions. *Nonlin. Dynam.* **2015**, *80*, 413–420. [CrossRef]
23. Wang, Y.; Zhang, F. Modeling and analysis of under-load-based cascading failures in supply chain networks. *Nonlin. Dynam.* **2018**, *92*, 1403–1417. [CrossRef]
24. Wang, J.; Liu, Y.H.; Zhu, J.Q.; Jiao, Y. Model for cascading failures in congested Internet. *J. Zhejiang Uni. Sci. A* **2008**, *9*, 1331–1335. [CrossRef]
25. Ren, H.P.; Song, J.; Yang, R.; Baptista, M.S.; Grebogi, C. Cascade failure analysis of power grid using new load distribution law and node removal rule. *Phys. A* **2016**, *442*, 239–251. [CrossRef]
26. Yin, R.R.; Liu, B.; Liu, H.R.; Li, Y.Q. The critical load of scale-free fault-tolerant topology in wireless sensor networks for cascading failures. *Phys. A* **2014**, *409*, 8–16. [CrossRef]
27. Shuang, Q.; Zhang, M.; Yuan, Y. Node vulnerability of water distribution networks under cascading failures. *Reliab. Eng. Syst. Saf.* **2014**, *124*, 132–141. [CrossRef]
28. Xu, X.; Zhu, Y.; Xu, M.; Deng, W.; Zuo, Y. Vulnerability analysis of the global liner shipping network: From static structure to cascading failure dynamics. *Ocean Coast. Manag.* **2022**, *229*, 106325. [CrossRef]
29. Sen, P.; Dasgupta, S.; Chatterjee, A.; Sreeram, P.A.; Mukherjee, G.; Manna, S.S. Small-world properties of the Indian railway network. *Physic. Rev. E* **2003**, *67*, 036106. [CrossRef]
30. Freeman, L.C. Centrality in social networks conceptual clarification. *Soc. Netw.* **1978**, *1*, 215–239. [CrossRef]
31. Zhang, G.; Wang, Y.; Li, Y.; Wang, S. An Analysis of the Impact of Russia Ukraine Conflict on China-Europe Railway Express. In Proceedings of the 2022 3rd International Conference on Big Data Economy and Information Management, Zhengzhou, China, 13 December 2022.
32. Notteboom, T.; Haralambides, H.; Cullinane, K. The Red Sea Crisis: Ramifications for vessel operations, shiping networks, and maritime supply chains. *Marit. Econ. Logist.* **2024**, *26*, 1–20. [CrossRef]
33. Xu, Y.; Peng, P.; Claramunt, C.; Lu, F.; Yan, R. Cascading Failure Modelling in Global Container Shiping Network Using Mass Vessel Trajectory Data. *Reliab. Engin. Syst. Safety* **2024**, *249*, 110231. [CrossRef]
34. Jiang, L.; Wang, G.; Feng, X.; Yu, T.; Lei, Z. Study on cascading failure vulnerability of the 21st-century Maritime Silk Road container shiping network. *J. Trans. Geogr.* **2024**, *117*, 103891.