algorithms

MDPI

Article

Vulnerability Analysis of a Multilayer Logistics Network against Cascading Failure

Tongyu Wu [1,*], Minjie Li [2] and Shuangjiao Lin [3]

[1] School of Traffic and Transportation, Fujian University of Technology, Fuzhou 350118, China
[2] School of Economics and Trade, Fujian Jiangxia University, Fuzhou 350108, China
[3] Institute of Economics and Management, Xiamen University of Technology, Xiamen 361024, China
* Correspondence: wty@fjut.edu.cn

Abstract: One of the most challenging issues in contemporary complex network research is to understand the structure and vulnerability of multilayer networks, even though cascading failures in single networks have been widely studied in recent years. The goal of this work is to compare the similarities and differences between four single layers and understand the implications of interdependencies among cities on the overall vulnerability of a multilayer global logistics network. In this paper, a global logistics network model set as a multilayer network considering cascading failures is proposed in different disruption scenarios. Two types of attack strategies—a highest load attack and a lowest load attack—are used to evaluate the vulnerability of the global logistics network and to further analyze the changes in the topology properties. For a multilayer network, the vulnerability of single layers is compared as well. The results suggest that compared with the results of a single global logistics network, a multilayer network has a higher vulnerability. In addition, the heterogeneity of networks plays an important role in the vulnerability of a multilayer network against targeted attacks. Protecting the most important nodes is critical to safeguard the potential "vulnerability" in the development of the global logistics network. The three-step response strategy of "Prewarning–Response–Postrepair" is the main pathway to improving the adjustment ability and adaptability of logistics hub cities in response to external shocks. These findings supplement and extend the previous attack results on nodes and can thus help us better explain the vulnerability of different networks and provide insight into more tolerant, real, complex system designs.

Keywords: cascading failures; multilayer logistics networks; vulnerability; complex network theory; topological feature; global

Citation: Wu, T.; Li, M.; Lin, S. Vulnerability Analysis of a Multilayer Logistics Network against Cascading Failure. *Algorithms* **2024**, *17*, 414. https://doi.org/10.3390/a17090414

Academic Editor: Frank Werner

Received: 15 July 2024
Revised: 30 August 2024
Accepted: 11 September 2024
Published: 19 September 2024

1. Introduction

Globalization is a process of economic, political, and cultural integration based on the global flow and allocation of production factors, which not only deepens the international division of labor and promotes global economic growth and international trade expansion but also strengthens the comprehensive connection of countries and regions in transportation, logistics, information, and finance, making it one of the most important collaborative endeavors of our time. While logistics activities are globally dispersed, the reorganization of resources in the network promotes agglomeration and the flow of capital, resources, technology, labor, production, and consumption to the most efficient place to connect supply and demand—the logistics hub city. As an important distribution place for goods circulation in a regional logistics network and a basic carrier of logistics development, a logistics hub city assumes the functions of factor resource exchange, organization, and service and can be an anchor of local development, as well as an important factor that enables a locality to integrate into global industrial and supply chains and participate in global value chain competition.

At present, there is no uniform definition of a "logistics hub city". However, some large ports, airports, railroad terminals, road freight stations, and other logistics infrastructure located in the city are essentially playing the function of logistics hub city.

On the one hand, the logistics hub city resides in the logistics network system and has the attribute of flow relationship. The attributes of a logistics hub city are not dependent on its own large scale and strong economic strength, nor the existence of logistics centers and logistics clusters, but on the network connection. The logistics hub city, from the network perspective, is not only the result of the flow relationship but also the main source of flow generation. The level of mobility relations determines the network status of logistics hub cities, which show more extensive and intensive interactions with other cities among all cities embedded in the logistics network system. The level of centrality is the basis of the important status of logistics hub cities in the network. The more central a logistics hub city is, the more it is in a position of important control in global logistics activities, and it becomes a basic node of important status in the logistics network and a spatial carrier of modern logistics activities, while other cities only act as ordinary nodes.

On the other hand, the influence and power generated by logistics hub cities change dynamically with the degree of their network connections. The influence and power of logistics hub cities lies in linking logistics activities at different geographical scales into the logistics network to realize resource flow and rational allocation, i.e., logistics hub cities act as the governance point of cross-regional activities to collect and disperse logistics activities manage and control them. For example, the specialized services of the agglomeration logistics companies and the logistics resources of the region are used as the control point of the logistics network system, and the producers located therein are used as the entry point of the global economy, so as to promote the large-scale flow and allocation of the elements of the global logistics resources through the relationship between the upstream and downstream enterprises of the supply chain and the synergistic relationship between the logistics companies, and so on. This means that functional institutions directly or indirectly involved in logistics activities in logistics hub cities are realizing the influence and power of logistics hub cities to promote the flow and rational allocation of logistics resources. In addition, the influence and power of logistics hub cities are not in a static state, and there are two aspects of dynamic changes with the network status:

a. The rise or fall in absolute change is manifested in increases or decreases in connectivity, control, breadth of linkage, and intensity of linkage.

b. The relative change of enhancement or decline is manifested in the fact that even if it maintains its original level of centrality or even improves it, it may still be in a state of relative decline along with the increase in the level of centrality of other cities. All of the above changes will affect the influence and power of the logistics hub city to change and alter its position in the logistics network system.

The above two connotations constitute the paradigm of a logistics hub city and thus analytically define a logistics hub city: a logistics hub city is a basic node city based on the logistics network connection, realizing the flow and allocation of resource elements, and dynamically exerting influence and power. Vulnerability is one of the fundamental properties of complex systems. Incidents or attacks can cause the collapse of logistics systems, such as natural disasters such as typhoons, targeted attacks such as destruction of the economy and trade, or even overload lines due to poor node capacities. An attack can cause great damage across cities worldwide and their surrounding regions (hinterlands). Taking economic and trade destruction as an example, a trade war between two countries will inevitably be accompanied by a reduction in trade orders and then cause a reduction in logistics demand. In a global logistics network, cities may face the problem of excess capacity and freight rates. In addition, due to a trade war, the market would continue to have a negative impact; thus, cities could even fail, and freight volume could plummet. Moreover, overloading cities may cause other kinds of problems. For instance, in the past 20 years, approximately half of all recyclables in the world have been shipped to China. However, beginning in July 2017, China announced that it would no longer accept

24 kinds of solid waste imported from other countries. As a result, large amounts of solid waste were transferred to other countries. Vietnam has already handled thousands of foreign containers containing solid waste, resulting in a shortage of support at Cat Lai. That shortage has caused more than 1000 containers to remain in the port of Cai Mep, adversely impacting port operations. Therefore, Vietnam decided to suspend the import of waste plastics and restrict the import of waste paper. As a result, Thailand, Malaysia, and Indonesia may be overloaded due to the large volume of waste imported from China. The impacts of this event have been amplified due to the interdependencies of cities, which are causing cascading failures.

Cascading failures are common and have recently received much attention. Localized failures or attacks on nodes can cause cascading failures and ultimately lead to the breakdown of a whole network, as widely researched in different types of networks [1]. This includes model descriptions [2–4], strategies for control or defense [5], and scenarios in real networks such as power grids [6–8], transportation infrastructure [9,10], and social networks [11,12]. In addition, the model was extended considering flows in interconnected networks or interdependent networks [13,14]. Furthermore, the definition of vulnerability may vary in different research areas. In general, vulnerability is defined as a property that makes the structure and function of a system susceptible to changes due to its sensitivity to disturbances. In this paper, vulnerability is measured by the decrease in efficiency from its original state after the disruption. A network is considered vulnerable if it changes sharply and suffers large cascading failures due to its properties. For strategies, attacks on nodes and edges have been widely used. Specifically, nodes or edges can be removed by the rank of degree [15], betweenness [16], eigenvector [17], PageRank [18], link [19], or path [20].

In logistics networks and even supply chain networks, the vulnerability of cascading failures is common, such as cascading failure modeling for logistics networks based on the local information of nodes [21,22], cascading failure propagation in logistics systems [23], cascading failure in evenly distributed logistics support networks [24], and importance evaluations of nodes under cascading failures of logistics infrastructure [25]. In addition, the mechanism of vulnerability in a logistics service supply chain was also researched [26,27]. However, compared to single networks, multilayer network models can better represent real-world systems. With the reshaping of global logistics networks, seaports and airports are engaged in international trade [28]. The interactions among networks have increasingly become intensive and complicated. It is a given that in multilayer global logistics networks, cities of a single layer are interdependent or interconnected to cities in other layers. Examples of multilayer networks can be found in different complex network research. In maritime areas where networks of ports interact with each other, Kaluza et al. researched the global shipping network as a multilayer structure consisting of three types of freighters [29]. Ducruet analyzed the interdependence between maritime networks and different commodity flows [30]. Tsiotas further introduced socioeconomic factors to converge the ports to regional administrations [31]. In air cargo networks, where airports are interdependent, Cardillo regarded the top 15 airlines in Europe as 15 levels, establishing a European aviation network [32]. The organization of a logistics enterprise network is mainly devoted to the analysis and comparison of the degree and connection between cities and is tightly integrated with the construction of urban networks [33]. Alternatively, in an international trade network, Calatayud et al. introduced indicators such as infrastructure and trade facilitation to construct a trade network and its support network [34]. These studies have suggested that a multilayer network connects different cities on different scales. In fact, a collapsed node in a multilayer network can cause more damage than a single node in a logistics system. Besides, the global and heterogeneous characteristics of networks could have a significant impact on the vulnerability of large systems and strategies to limit the spread of failures [35]. The correlation between heterogeneous logistics networks makes a logistics system more vulnerable while being more powerful and thus facing greater risks. When two or more subnetworks are interdependent, a fraction of city failures in one layer can trigger a cascading failure phenomenon that propagates in a multilayer global logistics

network. New aspects of the vulnerability of networks emerge when interdependencies of different layers are considered.

In the research on the vulnerability of cascading failures, the highest load or the lowest attack strategy was found. The highest load attack is often directed at nodes with the greatest connectivity or load. This strategy is based on the rationale that by targeting the most critical nodes, the overall network robustness can be significantly diminished [36]. Conversely, the lowest load attack, sometimes overlooked in comparison, targets nodes with the least load. This approach may not immediately impact the network's core functionality but can lead to a gradual degradation of network performance over time [37].

Recent studies have indicated that the effects of these attack strategies on the network are closely related to tunable parameters. For instance, the attack on edges with lower loads can result in larger cascading failures than those with higher loads under certain conditions [38]. Moreover, in the context of interdependent networks, the coupling strength between networks can influence the effectiveness of these attacks. When the coupling strength is weaker, attacking edges with a lower load can be more detrimental than attacking nodes with a higher load. However, this relationship reverses when the coupling strength is stronger [39].

The research also highlights the importance of local load redistribution in assessing network vulnerability. For example, in the US power grid, a reduction in the initial load can affect the critical threshold of the tolerance parameter differently depending on whether the attack is on the highest load nodes or the lowest load nodes. This finding underscores the need for a nuanced understanding of attack strategies and their potential impact on network performance [40].

As discussed above, the vulnerability of cascading failures is an important and active research field of multilayer networks that shows different structural characteristics and practical implications compared to single networks. However, the increasing research on vulnerability brings new questions. A major challenge is the design of a multilayer network to converge different logistics sublayers using the interdependencies of cities, such as the degree of overlap among the different layers of circulation composing global maritime flow [41]. However, most research is still limited to the assumption that one network does not have any connection with another network. Maritime transport, air transport, business organization, and international trade all have important respective roles in the development of cities, and sometimes the four are complementary. As long as network layers are constructed due to logistics hub city node connections, any changes observed between the topologies of the different layers illustrate the impact of network layer dependencies on node connections. Because attacks are rarely limited to a single layer in reality, the other question concerns the mechanism of cascading failures on the overloaded node of multilayer networks and how far the overload will affect the surrounding nodes. In particular, most articles have focused on modeling, and few of them are networks in the real world. In these models, the initial load is determined by the degrees and a parameter [42–44]. Their results could be more convincing if they simulate the load in the real world.

Therefore, this paper aims to fill part of this important research gap by converging different single networks, including a maritime network, air cargo network, logistics enterprise organization network, and international trade network. In addition, a load redistribution algorithm is introduced, where a weighted degree is used as the initial load, and a capacity parameter is used as the capacity of the load. Using the normalized metric of efficiency, the different attack scenarios include attacking the most important node and the least important node. As mentioned above, the subnetwork and even the converged network are compared. Furthermore, the primary contribution of the study is not only to extend classic notions to analyze the vulnerability of a multilayer network but also to make it possible to capture the properties of real multilayer logistics networks.

The rest of this paper is organized as follows. In Section 2, the model and data applied to the global logistics network are briefly described. It also describes attack strategies,

especially cascading failures, using a load algorithm. The topological metrics are also contained. In Section 3, the topological properties of the global logistics network, such as being scale-free and small world, are described. In Section 4, a vulnerability analysis presents the results for the single-layer networks and the multilayer network. It also discusses the implications of these results for vulnerability in the global logistics network. Finally, the summaries and conclusions are shown in Section 5.

2. Methodology and Data

2.1. The Model

As cities exist in one or more relationship systems, there is a type of differentiation in their links, and an analysis of the network location of city nodes can start from the links between cities. In terms of spatial organization, a logistics hub city network can be deconstructed into three levels: the physical network of infrastructure, the organizational network, and the trade flow network. Due to the diversification of facility types and organization levels of the physical network, the connection between node cities within the network is accordingly manifested in five forms, including a maritime transportation network, air cargo network, logistics enterprise organization network, international trade network, and integrated logistics network. These five types can be further summarized into two aspects: (1) The connection of the operation trajectory. This form of connection is mainly reflected in the occurrence of marine transportation, air cargo, and other logistics hub cities. Logistics transport between such cities does not rely on the geographic and spatial distribution of the line facilities, and its operational form is mainly expressed in the transport routes of the running track, such as maritime liner routes and air cargo flight routes. The measurement of this relationship is mainly through the number of route flights, frequency, and spatial geographic distribution. (2) The virtual connection of the "flow relationship". Such logistics hub cities do not rely on tangible route facilities or invisible trajectory routes but mainly consist of the relationship flows among cities, such as logistics enterprise headquarters branch relationships and international trade relationships. Therefore, this paper selects the maritime transportation network, air cargo network, logistics enterprise organization network, international trade network, and comprehensive network as the main source of research and analyzes the network corresponding to the five types of logistics hub cities: a port-type logistics hub city, air logistics hub city, organization logistics hub city, trade logistics hub city and comprehensive logistics hub city.

A city network structured with four distinct layers—Maritime Shipping Network, Worldwide Air-transportation Network, Logistics Enterprise Organization Network, and International Trade Network—reflects the multifaceted and interconnected nature of global urban systems. Each layer serves a unique purpose, and collectively, they form an integrated system facilitating the flow of goods, services, and information.

Maritime Shipping Network: This layer represents the global network of seaports and the maritime routes that connect them. It is fundamental for international trade, as the majority of global trade by volume is transported via sea. The maritime network is characterized by its hub-and-spoke system, where major ports act as hubs, and shipping lines connect these hubs to various spoke ports around the world.

Worldwide Air-transportation Network: This layer encompasses the global network of airports and air routes. It is crucial for the rapid transportation of high-value goods. The air transportation network is notable for its dense connectivity, especially among major economic centers, and plays a critical role in global economic integration.

Logistics Enterprise Organization Network: This layer involves the internal and external logistics operations of enterprises. It includes the coordination of activities such as transportation, storage, and distribution within a company and across its supply chain. The efficiency of this network is key to the competitive advantage of logistics enterprises and the overall performance of the supply chain.

International Trade Network: This layer represents the web of trade relationships between cities. It includes the exchange of goods, services, and capital and is indicative

of the economic interdependence among cities globally. The International Trade Network is characterized by its complex structure, reflecting the scale of trade and the diversity of economic activities.

The existence of these four layers in a city network acknowledges the complexity of modern urban systems and the need for an integrated approach to understanding urban dynamics. Each layer contributes to the overall connectivity and functionality of the city network, enabling it to respond effectively to the demands of globalization. Understanding the interactions between these layers is essential for effective urban planning, logistics development, and the enhancement of city competitiveness.

An integrated logistics hub city includes at least two attributes of a single-factor network, such as a combination of port-based and air-based logistics hub cities. Since the role of a logistics hub city network diffuses through city connections, this paper emphasizes not only the hub facilities radiating from routes in the transportation network, such as airports and seaports but also the placement of logistics firms in the city and the city's trade-generating capacity. The trade generating capacity reflects the intercity trade relations, the size and function of the logistics hub city itself, and its location, while the location of hub facilities and logistics firms reflects the city selection preferences of carriers in the logistics transportation system to emphasize the additional level of activity that geographic location conveys to the logistics hub city. Therefore, the networks characterized by maritime transport, air transport, logistics company organization, and international trade flows are constructed from three domains: a physical network, organizational network, and trade network, respectively, to serve trade and mobility through different functional roles. The integrated network is considered a logistics system consisting of interdependent and complementary subnetwork layers serving international trade and goods flows, and each subnetwork layer is considered an independent system or network.

The analysis of the global logistics network is considered a four-dimensional configuration. $G_{\Pi}(\Pi = a, b, c, d)$ is defined as four different kinds of single layers, which are closed contact through co-owned cities. The principle of construction is as follows: four single layers G_a, G_b, G_c and G_d of a multilayer network $M(G = \{G_{\Pi}, \Pi \in \mathbb{N}\}, C)$, the transformation of the form $g_x : G_i \to G$, where x is regarded as a given topological metric, such as degree, G is the family of the layers, and C is the connections between different layers. In this context, the set $T_G = \{g_X : X\}$ X is defined as the attribute of the network, which represents the effects of network topology caused by the node converging. The structure of single layers is modeled as a graph of N_{Π} nodes. The single layer $G_{\Pi} = (V_{\Pi}, E_{\Pi}, W_{\Pi})$ is composed of a set of city nodes V_{Π} and a set of edges E_{Π} between them. The weighted matrix W_{Π} is defined as follows.

$$W = \begin{bmatrix} 0 & W_{12} & \cdots & W_{1(n-1)} & W_{1n} \\ W_{21} & 0 & \cdots & W_{2(n-1)} & W_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ W_{(n-1)1} & W_{(n-1)2} & \cdots & 0 & W_{(n-1)n} \\ W_{n1} & W_{n2} & \cdots & W_{n(n-1)} & 0 \end{bmatrix}$$

The four single layers are characterized by a maritime network, air transportation network, logistics enterprise organization, and international trade network, as shown in Table 1.

Table 1. The meaning of the subnetwork and its node.

Mark	Name	Notes
G_a	Maritime Shipping Network, MSN	Container liner route to the port city
G_b	Worldwide Air-transportation Network, WAN	Air cargo transportation directly to the airport city
G_c	Logistics Enterprise Organization Network, LEN	Logistics company headquarters and branch city
G_d	International Trade Network, ITN	International trade import and export city

In addition, the link overlap coefficient is introduced to analyze the connections between different subnetwork layers. Specifically, the similarity between layers in a multilayer network can be measured by the number of common links, and the more connections there are between layers, the more similar the structure of the layers. The overlap coefficient between subnetwork layers Π and Π' is defined as [45]:

$$O_{\Pi\Pi'} = \sum_{i=1}^{n} a_{\Pi ij} a_{\Pi' ij} \tag{1}$$

where in subnetwork layers G_{Π}, node i links to node j, then $a_{\Pi ij} = 1$; otherwise, $a_{\Pi ij} = 0$.

2.2. Attack Strategies

There are two types of attacks in complex networks: random failures and targeted attacks. Random failure means that the node is attacked with a certain probability. In addition, targeted attacks mean that the nodes are attacked according to certain strategies. It is usually necessary to use the topology properties of the network, such as the importance of each node. Then, the most important node is selected as the first attack object. Furthermore, load attacks considering cascading failures assume that when a node fails, all edges connected to the node are deleted. If a city in a multilayer network is attacked, nodes based on shipping, air transportation, corporate organization networks, and trade flows will be removed (Figure 1).

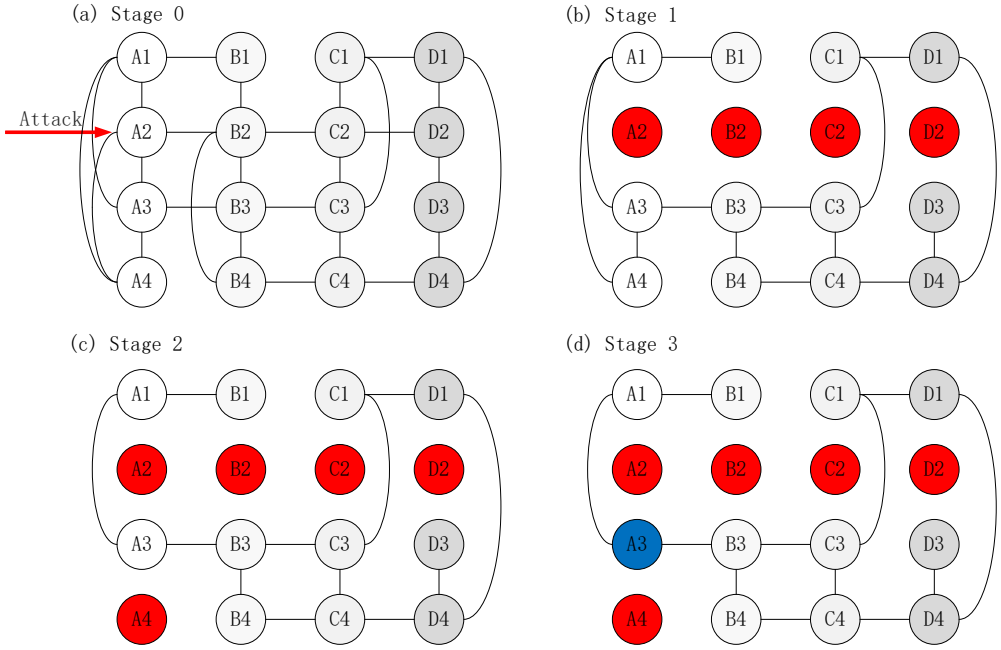

Figure 1. Schematic description of cascading failure between a single-layer or multilayer network. (**a**) Assume that node A2 has the largest load; therefore, A2 can be seen as the initial attack object. (**b**) When node A2 fails in network A, disconnect A2 from nodes A1, A3 and A4 and then fail between networks B2, C2 and D2. Then, redistribute the load of A2, B2, C2 and D2 within the network; namely, the load of the adjacent node increases. (**c**) Only the load distribution of the A2 node is considered here; that is, A1, A3 and A4 are adjacent to node A2. When there is more than one node of the same distance to A2, A4 is randomly selected to share the load of A2. If load A4 exceeds its capacity after the distribution of the load, then A4 will also fail. (**d**) After A4 fails, A3 is selected to share the load. If the load of A3 does not reach its capacity and is retained, then the cascade fails. The efficiency of the network could be calculated.

2.2.1. The Initial Load Distribution and Capacity of the Node

In the cascading model, the initial distribution of load L_i is based on the importance of node i [46]. Then, the initial load of node i is usually defined as

$$L_i = \rho k_i^{\xi} (\xi > 0) \tag{2}$$

where k_i is the degree of node i. ρ is a constant. ξ is a tunable parameter that is used to control the strength of the initial load of node i in the network. Since the logistics hub city has the characteristics of fast-in and fast-out and large transit volume, the weighted degree centrality is consistent with this characteristic. Therefore, the strength of node i, that is, the weighted degree centrality, is taken as the initial load of node i.

$$L_i = k_{wi} \tag{3}$$

where k_{wi} is the weighted degree centrality of the node.

The capacity C_i of node i is determined following the ML model [1], assuming that the capacity is proportional to its initial load, namely,

$$C_i = L_i(1 + \alpha)(0 \leq \alpha \leq 1) \tag{4}$$

where α is the capacity parameter that represents the capacity or tolerance of the network in cascading failures. The smaller the capacity parameter is, the more sensitive the urban node is to the change in logistics volume, while a larger capacity parameter indicates that the city is basically not affected by the distribution of logistics volume in other cities.

2.2.2. Load Redistribution Algorithm

The iteration rule against cascading failure with the following algorithm. After a given node i, with the highest load, or the lowest is attacked, the load will be assigned to its neighboring nodes with certain rules, resulting in an update of L_{ji}

$$L_{ji} \to L_{ji}{}' = L_j + \Delta L_{ji} \tag{5}$$

After node i fails, the load obtained by the adjacent node is defined as

$$\Delta L_{ji} = L_i \cdot \frac{C_j}{\sum\limits_{m \in \Gamma_i} C_m} \tag{6}$$

where Γ_i represents the set of all the neighboring nodes of node i, m represents any node in the set, and C_j and C_m represent the capacity. If $L_j + \Delta L_{ji} > C_j$, then node j will also fail. The rest of the load will be distributed by the above rules until the failure node no longer appears. Assigning the load to the neighboring nodes is a partial redistribution mode because the neighbor of the failed node may continue to load. The transfer between intact nodes in the network, that is, the distribution of the nodes, is a global behavior.

2.2.3. Iterative Steps for Cascading Failure

The iterative steps for cascading failure are shown in Figure 2.

Step 1. At the initial moment, a given node will be removed (maximum load/minimum load).

Step 2. Update the load of the nodes.

Step 3. Check if the node load exceeds its capacity. If it is overloaded, remove the node; otherwise, keep it.

Step 4. Repeat steps 2 and 3 until the node with sufficient capacity in the network sustains the load of the failed node. At this time, the network reaches a steady state, and the cascade fails. Then, the network efficiency and the avalanche size are calculated.

Step 5. Remove nodes one after the other and calculate the network efficiency and the avalanche size in order.

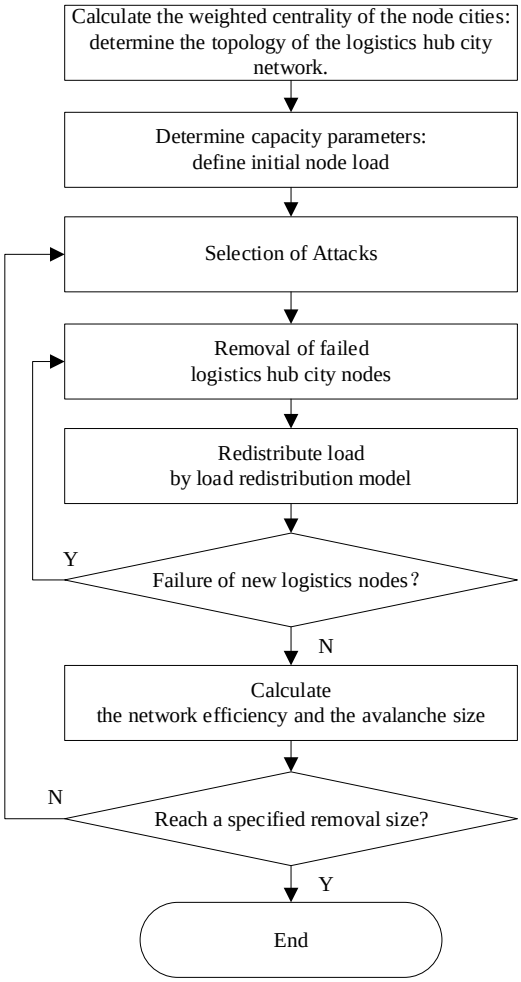

Figure 2. Iterative steps for cascading failure.

2.3. Topological Metrics

Network efficiency is used to analyze the performance of the network, which could capture the difficulty of reaching the distant part of the network and the ability to share the flow and information. Improving network efficiency is a potential way to improve network reliability in reality. The vulnerability is associated with an attack and can be measured by a reduction in efficiency after that.

Network efficiency is an important evaluation index of the network operation effect, reflecting the ease of materials from a specific city to reach the network farther away, used to measure the efficiency of the exchange of materials between cities. In practice, container liner companies or air cargo companies choose to open routes by not only considering the geographical distance between cities but also taking into account the demand for cargo transportation, the number of empty containers, transit costs, transportation conditions, and other factors. Therefore, instead of expressing the transportation distance between logistics hub cities in terms of traditional geographical distance, the minimum number of transit times connecting two logistics hub cities is used, i.e., the number of sides to be passed by the shortest path between the two cities is used to express the distance of city i and j. Because the efficiency of transmission between the two logistics hub cities ε_{ij} is

inversely proportional to the distance of the shortcut, $\varepsilon_{ij} = 1/d_{ij}$ when $d_{ij} = \infty$, $\varepsilon_{ij} = 0$ [47]. The network efficiency is defined as:

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

where n is the total number of cities in the network and d_{ij} is a shortcut distance between cities. The inverse of the distance is set as the transmission efficiency between two cities, and the network efficiency is expressed as the average of the transmission efficiency between any two logistics hub cities in the network. If the shortcut distance is too large, the network efficiency is lower, which will affect the transmission of information and the flow of elements in the network, in which the transmission efficiency and diffusion of logistics hub cities are weaker, and the response speed to external disturbances lags and slows. In contrast, the smaller the shortcut distance is, the higher the network efficiency and the stronger the global connectivity and transmission performance of the network. The logistics hub city can realize the flow of goods at a relatively low cost and relatively fast, and it can enhance the resistance of the logistics hub city to external risks.

Avalanche size is a measure of the degree of damage to network efficiency under the city node disruption scenario and is the proportion of the number of failures of a particular logistics hub city until the end of the cascade failure process will cause the failure of other nodes in the network to the number of cities in the initial state, defining the avalanche size as

$$\delta = 1 - \frac{N^*}{N} \tag{8}$$

where N and N^* are the number of cities in the network that can maintain normal operation before and after the cascade failure phenomenon. The larger the avalanche, the greater the damage to the overall network of logistics hub cities.

Different topological metrics describe a specific structural characteristic of the global logistics network. In this work, we consider the following metrics.

The degree k of a node is the number of edges linked with the others in a network [48].

$$k = \sum_{j=1, j \neq i}^{n} X_{ij} \tag{9}$$

where X_{ij} is the number of links between node i and node j, and n is the total number of cities.

The weighted degree k_w is an extension of the degree k.

$$k_w = \sum_{j=1, j \neq i}^{n} w_{ij} \tag{10}$$

where w_{ij} is the weight of the links of the node i [49].

The cumulative degree distribution is defined as the degree distribution. $P(k)$ is the fraction of nodes with degrees greater or equal k.

$$P(k) = \sum_{k'=k}^{\infty} p(k') \tag{11}$$

For a network of n nodes, the average degree represents the average importance of nodes [50].

$$K = \frac{1}{n} \sum_{i=1}^{n} k_i \tag{12}$$

The average shortest path length L is defined as the average number of edges along the shortest path d_{ij}, which represents the separation of the nodes [51].

$$L = \frac{2}{n(n-1)} \sum_{i \neq j} d_{ij} \tag{13}$$

The diameter of a network is defined as the maximum value of all d_{ij} [52].

$$D = \max d_{ij} \tag{14}$$

The clustering coefficient Q_i of a node i is the portion of edges linked within its neighborhood divided by the maximal possible edges between them [53]. The average clustering coefficient is defined as

$$Q = \frac{1}{n} \sum_{i=1}^{n} Q_i \tag{15}$$

X' is the normalized value, X is the original value, $X_{\min}$ is the minimum value, $X_{\max}$ is the maximum value.

$$X' = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \tag{16}$$

2.4. Data

To compare and analyze the topological properties and vulnerability of the global logistics network, the following four kinds of data are collected (from January to August 2018).

(1) Container shipping data. Shipping companies with a business share of more than 1% are collected from Alphaliner (site: https://alphaliner.axsmarine.com/PublicTop100/ (accessed on 1 January 2018)). The companies above have a containerized volume accounting for 86% of the total global container volume, which is representative. In addition, the maritime data are derived from the cities in the shipping schedule of the company's website mentioned above. In order to standardize the scope of cities, cities with 2 or more ports are combined and extracted (e.g., there are 4 container ports in Shenzhen, namely, Shekou Port, Yantian Port, Chiwan Port, and Dachan Bay, which are simplified and combined into a unified calculation for Shenzhen).

(2) Air cargo data. Only the freight routes and airport cargo data are collected to measure the important relationship of freight airports in the global logistics network. The air cargo company is derived from Air Cargo World (site: https://aircargoworld.com/allposts/freight-50-top-50-carriers-chart/ (accessed on 1 March 2018)), and the data process is the same as the shipping network.

(3) Organizational structure of logistics companies data. The companies are selected according to the authoritative magazine of the North American Logistics Association, namely, Transport Topics (site: https://www.ttnews.com/top50/logistics/2017 (accessed on 1 March 2018)). The headquarters and branches of the top 50 global logistics enterprises are collected. In addition, a Taylor series chain model algorithm is introduced to research the production service industry. According to its standard of service value [54], the value matrix is constructed.

(4) International trade data. Compared to the previous research estimating trade flow [55], an airport cargo and mail throughput number is introduced. This part of the data is calculated by the proportion of total merchandise trade between countries, the proportion of each city's port container throughput in the country's total number, and the proportion of each city's airport cargo and mail throughput in the country's total number. Assuming that countries have the same foreign trade goods generation coefficients, simplify the formula to:

$$T_{ij} = TC_{uv} \cdot \frac{P_i}{PC_u} \cdot \frac{P_j}{PC_v} \cdot \frac{A_i}{AC_u} \cdot \frac{A_j}{AC_v} \tag{17}$$

where T_{ij} is the estimated value of merchandise trade (weights) from city i to country j, TC_{uv} is the merchandise trade from country u to country v, P_i is the container throughput at ports of city i, PC_u is the total port container throughput of country u, A_i is the cargo and mail throughput at airports of city i, AC_u is the total airport cargo and mail throughput of country u, U is the city aggregation of country u, Z is the city aggregation of country z. The data of this part are derived from Lloyd's List (site: https://lloydslist.maritimeintelligence.informa.com/markets/containers (accessed on 1 March 2018)), Air Cargo World, the World Bank (site: https://data.worldbank.org/ (accessed on 1 August 2018)) and the United Nations Conference on Trade and Development (UNCTAD) (site: https://comtrade.un.org/db/ (accessed on 1 August 2018)).

3. Topological Properties

3.1. Scale-Free

Using the formula defined by Equation (11), the degree cumulation distribution of the networks is calculated, as shown in Figure 3. The degree distributions of the four networks are different from each other. The maritime network (Figure 3a) fits more with the exponential distribution. In addition, the effect of fitting with a power function is more obvious than the exponential function in the air cargo network (Figure 3b) and the organization network (Figure 3c). The trade network in Figure 3d also seems to obey the power law distribution, while it does not have a good fit. Overall, it is suggested that among the four single networks, the scale-free properties are similar to $G_b > G_c > G_d > G_a$. The fitting curves for the degree cumulation distribution of the multilayer network are shown in Figure 4. The multilayer network still has the scale-free property ($y = 1094.474x^{-0.405}$, $R^2 = 0.918$). The global logistics hub city network is in the stage of complex and orderly structure, forming an overall large-scale network structure and gradually tending to mature. The polarization effect is a reflection of the scale-free network, thus affecting the uneven distribution of the centrality of logistics hub cities in the global space and prompting the phenomenon of geographical concentration of the links between logistics hub cities.

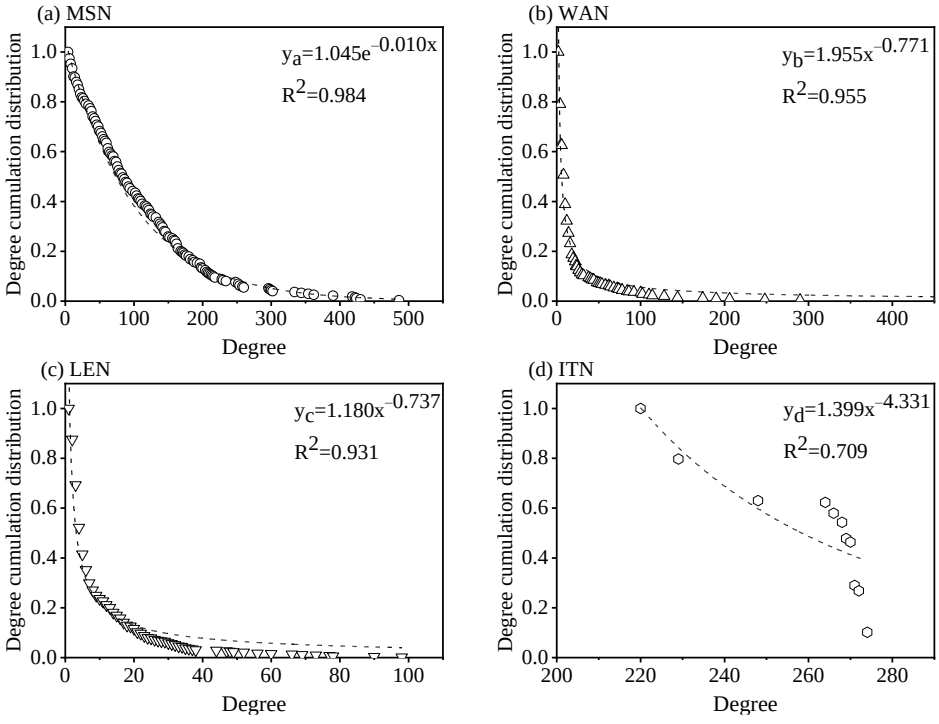

Figure 3. Fitting curves for the degree cumulation distribution of the subnetwork. (**b**,**c**) are consistent with a power-law behavior.

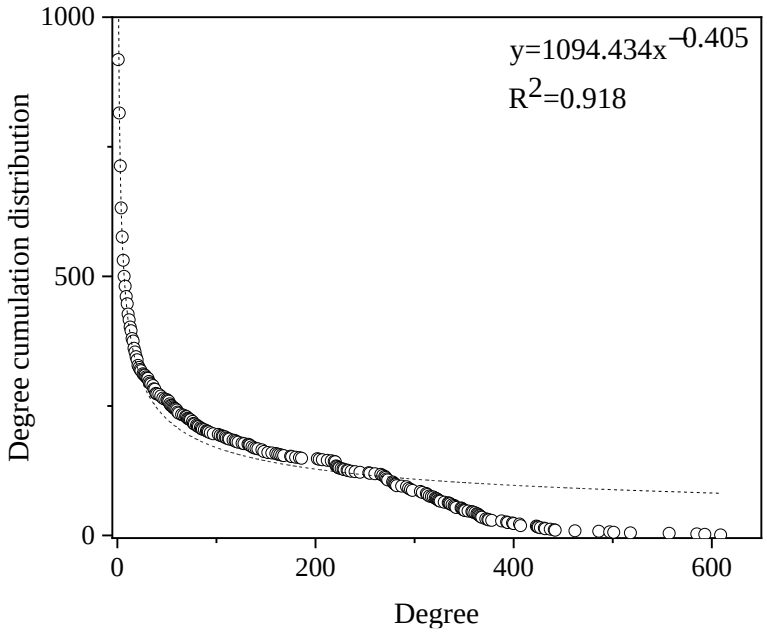

Figure 4. Fitting curves for the degree cumulation distribution of the multilayer network.

3.2. Small World

Small-world property is characterized by two indices. If the clustering coefficient of the network is significantly higher than the random graph of the same-scale structure of the nodes and has a similar and even small average path length, then the network has a small world characteristic. In Table 2, taking the MSN as an example, the agglomeration coefficient is 0.714, which is higher than the same-scale random network coefficient (0.378), and its average path length is 1.875, which is close to the same-scale random network path length (1.622). Similarly, to find the small-world index of other subnetworks, it can be seen that all four single-layer networks have small-world properties. That is, the subnetwork has a high degree of connectivity or strong agglomeration, and most of the nodes are connected to their neighbors. Overall, it is suggested that among four single networks, the properties of the small world are similar to $G_d > G_a > G_b > G_c$.

Table 2. Statistical characteristics of networks.

Metrics	G_a	G_b	G_c	G_d	G
Node	274	496	528	138	918
Average degree	106.17	16.69	4.19	126.53	35.19
Network diameter	4	6	10	2	6
Average clustering coefficient	0.714 (0.378)	0.687 (0.034)	0.259 (0.007)	0.927 (0.912)	0.546 (0.038)
Average shortest path length	1.875 (1.622)	2.710 (2.517)	3.698 (3.630)	1.076 (1.087)	2.550 (2.172)
Small world index	0.381	0.254	0.070	0.862	0.214

It is concluded that networks with small-world properties are evenly distributed. The number of links connecting different nodes is roughly the same. In addition, most nodes can reach any other nodes through a few associated nodes.

4. Vulnerability Analysis

4.1. Load Vulnerability

Based on the weighted centrality measurements, the top ten cities in different network layers with weighted centrality are shown in Table 3.

Table 3. Top 10 cities in terms of weighted centrality values in different network layers.

Network Layer	Top 10 Cities in Terms of Weighted Centrality Values
Maritime Shipping Network	Shanghai, Ningbo, Singapore, Shenzhen, Busan, Hong Kong, Qingdao, Klang, Rotterdam, Kaohsiung
Worldwide Air-transportation Network	Frankfurt, London, Hong Kong, Munich, Vienna, Dubai, Memphis, Miami, Shanghai, Cincinnati
Logistics Enterprise Organization Network	Shanghai, Singapore, Hong Kong, Dubai, Chicago, Dallas, Shenzhen, Miami, Basel, Cincinnati
International Trade Network	Shanghai, Hong Kong, Busan, Rotterdam, Singapore, Frankfurt, Paris, Vancouver, Hamburg, Le Havre
Multilayer Logistics Network	Singapore, Shanghai, Hong Kong, Klang, Frankfurt, Shenzhen, Busan, Ningbo, Rotterdam, Miami

The *X*-axis represents the capacity parameter, and the *Y*-axis represents the network efficiency. The capacity parameter increases from 0 to 1, with a step size of 0.1. The change in network efficiency with capacity parameters after cascade failure is analyzed using two node attack strategies: maximum load attack and minimum load attack. The simulation results of four single-network layers and comprehensive multilayer networks, namely, the maritime transport network, air transport network, logistics enterprise organization network, and international trade network, are given. As shown in Figure 5, (1) when the capacity parameter of the node is small, the network efficiency remains at a low state. With the increase in the capacity parameter of the node, the network efficiency is significantly improved. When the capacity parameters vary from 0 to 1, the network efficiency curve constantly decreases, and the reason for this is that with the increase in capacity parameters, the city's ability to bear the load will increase, the dynamic load distribution makes the load distribution uniform, cities will not be better able to bear the node load, and sensitivity to external disturbances will be reduced. When the capacity parameter increases to 0.5, the increase in capacity parameter enables the network efficiency to maintain a high state, leading to a reduction in network vulnerability and better connectivity performance of the urban network of logistics hubs. (2) Under different node attack strategies, the network efficiency is greatly different. In the case of a minimum load attack, due to the small load of failure node transfer, it is unable to cause a large-scale impact on other cities; that is, the network has strong resistance, and it is not easy to cause a cascading failure. For the maximum load attack, after the node with a larger load is removed, the original load will be distributed to other nodes in the network, and the intact node may be removed after receiving the load of the failed node, which may exceed its node capacity, thus causing the maximum loss of network efficiency. Even when the capacity parameter reaches the maximum, due to the increase in failure nodes, the connection of nodes in the network will decrease accordingly, and the realization of city interconnection requires longer links, which affects the network efficiency to some extent. Therefore, the nodes with high loads in the urban network of the logistics hub can maintain the efficient operation of the network, which should be protected to avoid serious damage to the network due to cascade failure.

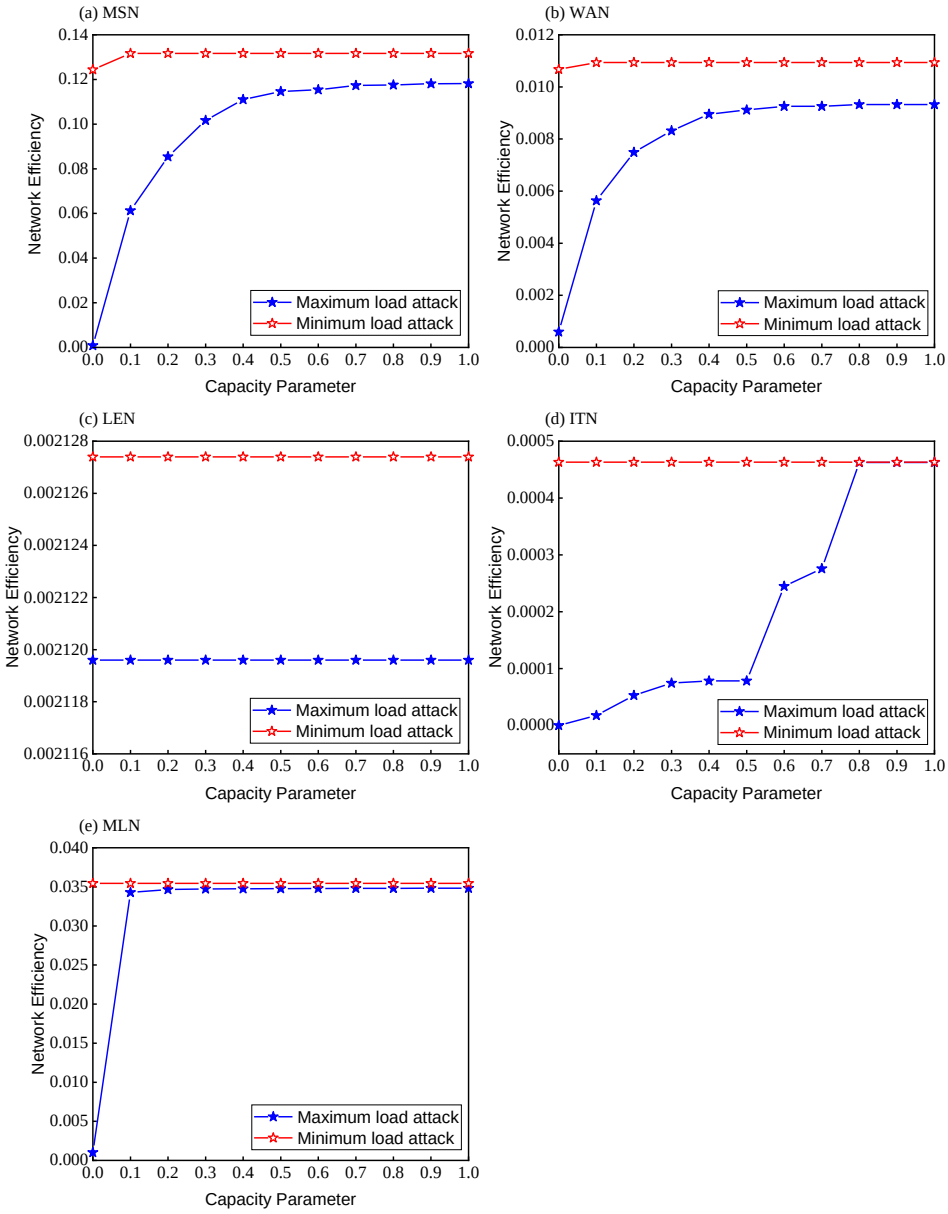

Figure 5. The network efficiency of different attack strategies varies with capacity parameters under cascade failure.

The X-axis represents the capacity parameter, and the Y-axis represents the avalanche scale. The capacity parameter increases from 0 to 1, and the step size of proportional growth is 0.1. The avalanche scale actually reflects the degree of damage to nodes. Under different capacity parameters, the maximum load and the minimum load attack strategies are adopted to calculate the avalanche scale of the network when the cascade failure reaches a stable state. The simulation results of four single network layers and comprehensive multilayer networks, namely, the maritime transport network, air transport network, logistics enterprise organization network and international trade network, are given. It can be seen in Figure 6 that (1) when the capacity parameter of the node is small, the attack on the node with the maximum load will cause a large avalanche scale, which will cause part of the network to not run normally. With the increase in the capacity parameter, the avalanche scale will obviously decrease, and only a few node cities may encounter failures. For example, when the capacity parameter $\alpha = 0.1$, the avalanche scale generated by the attack on the highest load node is more than 50%. The flow of each node in the network is close to the city's maximum capacity limit, which leads to the city's high sensitivity.

The disturbance will cause more nodes to be destroyed, leading to a large-scale cascade effect. When the capacity parameter $\alpha > 0.5$, the failure scale of the overload cascade gradually decreases, and the avalanche scale converges to 0, indicating that the network cannot trigger cascade failure or that only a few nodes can fail, which conforms to the rule that cascade failure damage decreases with increasing node capacity. Therefore, larger capacity parameters can avoid or slow down the occurrence of cascading failures. (2) Under different node attack strategies, the avalanche scale varies greatly. The attack method of removing the highest load causes more cascading failure nodes in the network than the lowest load, and the size of failure nodes generated is 0~40%. The avalanche scale curve generated by the attack on the lowest load node presents a curve parallel to the *X*-axis and infinitely approaching 0, indicating that under the attack mode of the lowest load, all the nodes except the attacked node can maintain the existing logistics function.

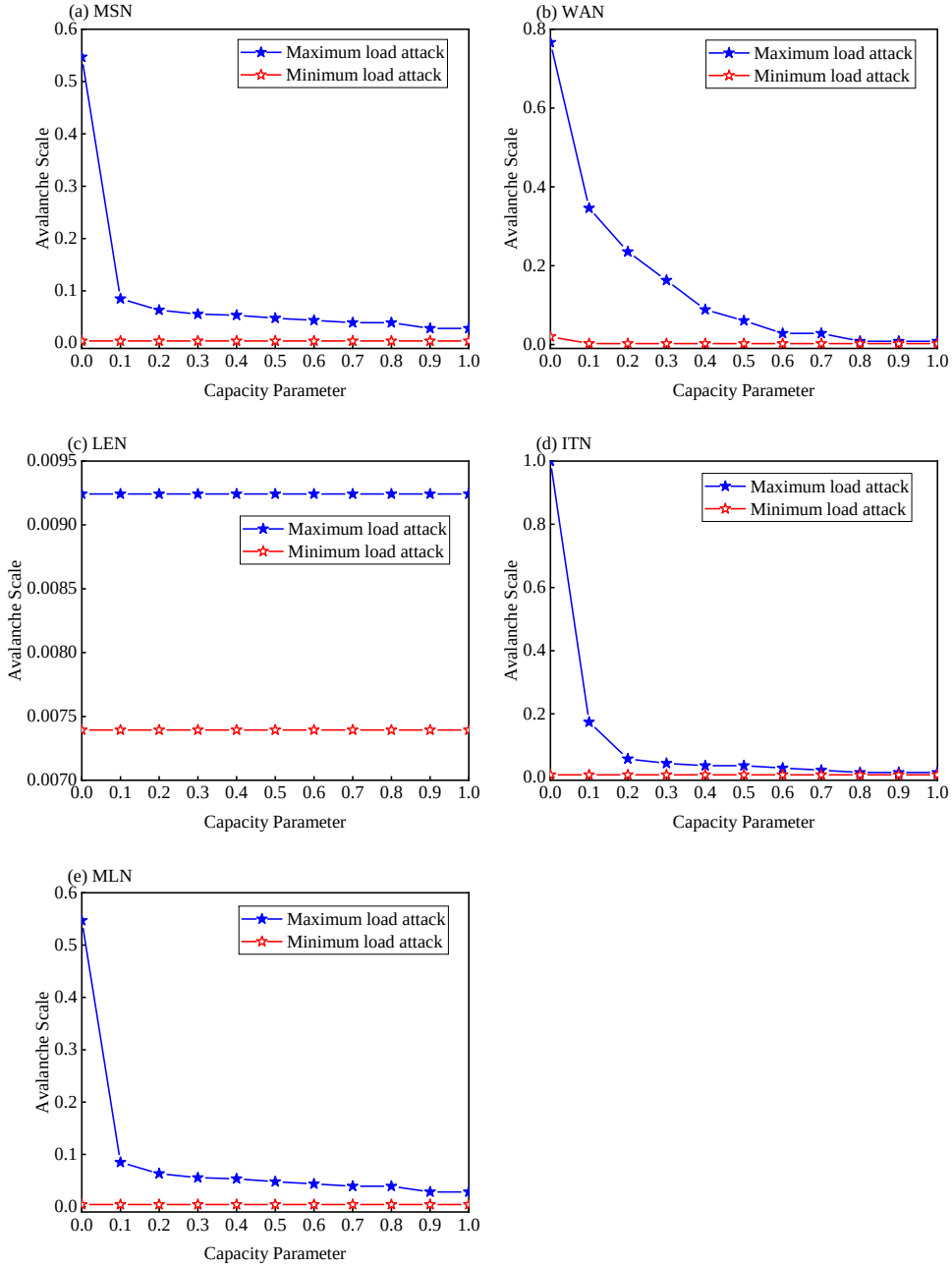

Figure 6. The avalanche size of different attack strategies varies with capacity parameters under cascade failure.

4.2. Structural Heterogeneity Vulnerability

The node with the maximum load is the most critical node in the network, and it plays a vital role in the timeliness and connectivity of logistics supply and demand between cities. After these critical nodes are attacked, isolated nodes will be generated on a large scale, which will lead to a change in network topology and a fast decrease in network operation efficiency. To study whether the characteristics of cascade failure are affected by network heterogeneity, the network efficiency of different network layers is normalized and compared. As seen in the Figure 7, when only a single network-layer node is removed, the decline rate of different network efficiency curves and the failure scale of nodes are different, which means that under the same attack strategy, the disturbance effect caused by different network structures is different.

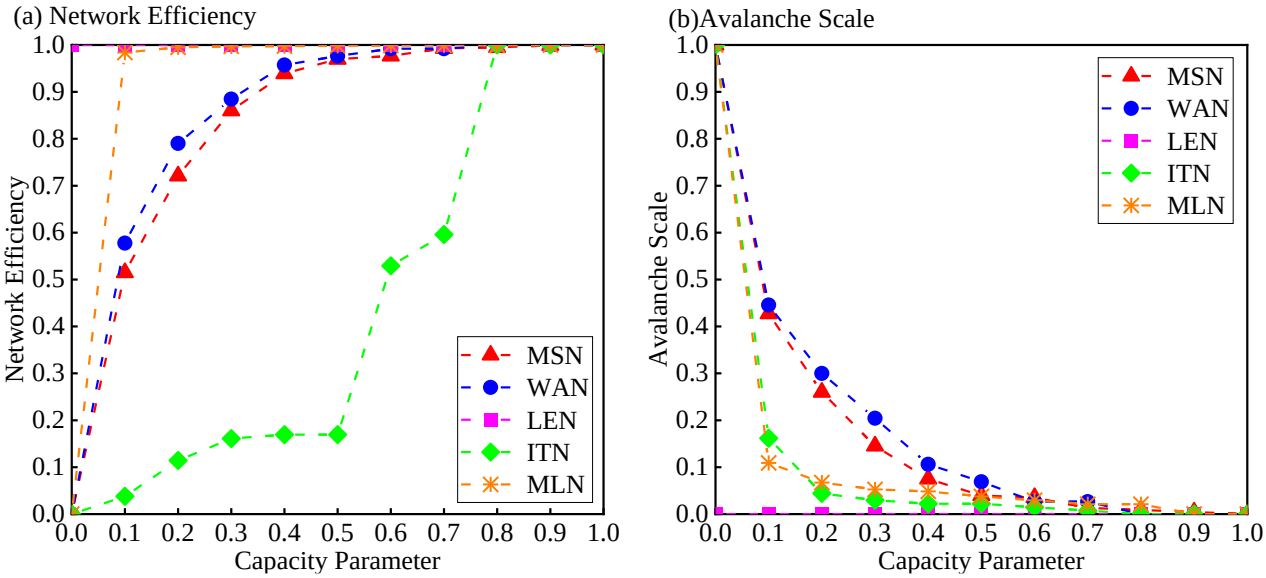

Figure 7. The network efficiency of different network layers varies with capacity parameters under cascade failure.

This is embodied in the following three aspects: (1) Compared with the result of a single network layer, the network efficiency in a multilayer network is larger. In each network layer, node failures are caused not only by traffic redistribution but also by the load transferred by congested nodes in another network layer that has dependencies. Therefore, the iteration of multiple networks amplifies the fault of a multilayer system and easily triggers the further expansion of the failure scale. However, due to the stability of the organizational network of logistics enterprises to attack, the failure speed of the multilayer network is slowed down to some extent, so the vulnerability of the multilayer network is reduced, and high network efficiency is maintained. (2) In the organizational network of logistics enterprises, regardless of the minimum load attack or the maximum load attack, the impact on the network efficiency is relatively gentle, indicating that the attack on nodes does not easily trigger a large-scale cascading failure phenomenon. The reason is that the organizational network of logistics enterprises has a small average clustering coefficient, the network structure is relatively sparse, and the nodes are not evenly distributed. In a sparse and uneven organizational network, only a few communities have cascading failures. The attacked nodes are distributed in different communities at the same time, and the load of the failure node is difficult to transfer between different communities. Therefore, the network characteristics of small clusters enable the organizational network of logistics enterprises to maintain the efficient operation of the global network, even if a small number of independent groups are damaged. (3) The small capacity parameter causes large-scale destruction of the network, and the destruction degree is affected by the density of the network and the structure of the network. When the capacity parameter

$\alpha = 0.1$ is used, the damage to the international trade network is serious, and the loss of network operation efficiency is higher than 90%. Maritime networks and air transport networks came in second, with a network efficiency and failure node size of nearly 50%, indicating that the smaller node carrying capacity allows an attack to destroy almost half of the network. The operational efficiency of the organizational network and multilayer network of logistics enterprises is relatively high. According to the above analysis of network topological characteristics, the international trade network, maritime transport network and air transport network all have high small-world characteristics, while the remaining networks are relatively sparse and non-uniform.

Combined with the small-world index (the ratio of the network clustering coefficient and average path length), the order of different network layers from large to small is as follows (Figure 7): $G_d > G_a > G_b > G > G_c$. Under the maximum load attack, the network efficiency varies from large to small: $G_c > G > G_b > G_a > G_d$. The ranking of avalanche size is as follows: $G_b > G_a > G > G_d > G_c$. It can be seen in the above ranking that the higher the small-world index is, the faster the network efficiency declines after being attacked. Therefore, it can be concluded that dense and homogeneous logistics networks tend to maintain higher connectivity under normal conditions, but if one city fails, other cities may not be connected, and half of the networks will be affected. In contrast, sparse and heterogeneous networks are more stable.

5. Discussion and Conclusions

Due to increasing globalization, urban socioeconomic linkages are becoming more complex, bringing unstable operating conditions and more difficult challenges to the global logistics system. Logistics hub city transmission performance is mainly maintained by a small number of key logistics hub cities, which have a greater degree of influence on the overall network operation efficiency. In the context of economic globalization, the tendency of spatial decentralization of logistics hub cities will further aggravate the spread of the impact of local logistics hub city disruptions to the external space. Therefore, a vulnerability simulation analysis of the impact of logistics hub cities on the network operation efficiency under the disruption scenario can help to predict the impact of the damage of logistics hub cities on the overall network efficiency to arrange a response in advance.

From the perspective of complex network theory, global shipping, air cargo, logistics enterprise organization, and international trade, four types of networks are built to analyze the single network and multilevel logistics hub city network cascade failure phenomenon. The main conclusions are as follows:

(1) Improving the size of urban capacity can effectively improve the operational efficiency of the urban network of logistics hubs. The capacity parameters are affected by the operational capacity of urban logistics. To strengthen the capacity of network components, it is necessary to increase the quick transfer capacity of logistics. However, from the perspective of the economy, the limitation of resources does not allow the expansion of all node capacity, and the expansion of node capacity will consume many logistics resources. However, if nodes do not bear a high load but use a high-capacity configuration, this will cause waste. Thus, there is a trade-off between function and economy.

(2) When high-load logistics hub cities are attacked, their network efficiency decreases faster, indicating that cities with a stronger hub nature have a greater impact on the overall network efficiency. However, in the actual operation process, overloaded logistics hub cities often appear. Due to the lack of sufficient resources and costs to ensure that all cities can maintain normal operations in case of emergencies, a reasonable resource allocation strategy can minimize the transmission scale of network cascade failure. Implementing targeted protection measures for key logistics hubs can avoid damage and waste of resources due to the expansion of all urban capacity. Multiple logistics hub cities should be established within a certain range to reduce the dependence on a single city and ensure the efficient operation of the network.

(3) Compared with dense and uniform network structures, sparse and heterogeneous network structures can better improve the stability of overall logistics network efficiency when some cities are damaged. The dense and homogeneous topological structure of the network itself leads to the excessive establishment of association relations between logistics hub cities and other cities, resulting in the high dependence of most cities on a few hub cities. After a few key hub cities are attacked and collapsed, they will have a huge negative impact on the overall logistics network structure. Therefore, for logistics systems with different topological structures, the capacity of nodes can be improved by increasing logistics processing resources to reduce the probability of functional failure of logistics hub cities and make the network more efficient.

(4) The vulnerability of a multilayer network lies in its network layer vulnerability. Once a key logistics hub city fails in an emergency or interference event, it will have a more profound impact on the damage resistance of a multitiered logistics hub urban network system. Therefore, it is an effective measure to improve the destruction resistance of the urban network system of logistics hubs and a potential way to improve the reliability of the network to strengthen the logistics coupling relationship between cities, increase the direct dependence of different network layers on functions and improve the complexity of the network structure.

Due to the diversity and uncertainty of risk sources for logistics hub cities, most of the impact and diffusion paths of risk shocks do not follow a regular pattern in advance. Therefore, the three-step response strategy of "Prewarning–Response–Postrepair" is the main pathway to improving the adjustment ability and adaptability of logistics hub cities in response to external shocks.

First, we should actively promote preventive medical examinations, risk monitoring and early warning mechanisms and strengthen the redundancy and modularity of infrastructure construction in logistics hub cities to identify the contingencies and risks that logistics hub cities may face, carry out security risk assessment of logistics hub cities, and form personalized physical examination reports of logistics hub cities to identify the shortcomings of logistics hub cities. The logistics needed during a crisis period should be considered to avoid the various risks faced by the logistics hub city proactively during the course of operation.

Second, action guidelines should be developed to promote active feedback and active response mechanisms during an attack event to enhance the logistics hub city's comprehensive emergency logistics security capacity. Governments at all levels should consider the resource endowment, network layout and emergency security of logistics hub cities and formulate action guidelines or action plans for emergency capacity building of logistics hub cities under the impact of emergencies, mainly involving short board identification, system construction, key technologies, policy initiatives and risk response checklists, such as optimizing the stock of logistics hub cities with the advantages of their network functions and trunk line transit capacity. The layout of emergency material reserve facilities thus reduces the losses caused by shocks to a minimum level. For example, Shenzhen, China, has maintained regular cargo flights, launched international air cargo charter services, and implemented measures such as "passenger to cargo" contribution to flight increase to cope with the impact of the COVID-19 epidemic.

Third, timely reflection and optimization should be promoted, and post-event repair and dynamic adjustment mechanisms should be actively promoted. On the one hand, it is necessary to introduce improved policies and initiatives and continuously absorb the lessons learned by itself and other cities in response to the crisis to reduce the vulnerability of logistics hub cities and improve the "immunity" and reliability of logistics hub cities in response to emergencies; on the other hand, it is necessary to improve the emergency response function of the comprehensive information platform and make use of big data technology for assessments. On the other hand, it is necessary to improve the emergency functions of comprehensive information platforms, make use of big data technology to evaluate whether there is a logistics supply gap or redundancy and its real logistics de-

mand, quantify and rank the urgency of supply and demand in terms of strategy, value and urgency, further realize the information sharing and cooperative operation ability of suppliers, logistics enterprises and government departments, promote matching resources and regulation processes, and improve the collection and deployment of materials, transportation and transit, distribution and delivery to ensure the normal operation of the logistics hub city under the risk impact.

The research offers an extensive examination of cascading failures within multilayer global logistics networks. However, the utilized cascade failure model may not fully capture the complexities of networks resembling tree structures. While the model's emphasis on the weighted degree as a critical node indicator is beneficial, it does not delve into alternative attack strategies, such as random or median attacks, which might offer further clarity on network vulnerability.

The robustness of multilayer global logistics networks should be a key focus in future research. Delving into recovery strategies after failures could expose the processes through which various cities recuperate from cascading effects, potentially leading to the creation of more resilient infrastructures. Moreover, future research should consider the spatial arrangement of nodes and its influence on the network's overall stability and strength.

In conclusion, future research should concentrate on models that address the wide-ranging facets of cascading failures, infrastructure resilience, and the capacity of logistics networks to adapt to growing demands and unforeseen disruptions.

Author Contributions: T.W.: Conceptualization, Methodology, Software, Investigation, Formal Analysis, Writing—Original Draft; M.L.: Modifications; S.L.: Modifications. All authors have read and agreed to the published version of the manuscript.

Funding: Social Science Foundation of Fujian Province (No. FJ2023C046). Education and Research Project for Young and Middle-aged Teachers of Fujian (Social Science) (No. JAS22089).

Data Availability Statement: The datasets generated and analyzed during the current study are not publicly available because they constitute an excerpt of research in progress but are available from the corresponding author on reasonable request.

Conflicts of Interest: All authors disclosed no relevant relationships.

References

1. Motter, A.E.; Lai, Y.-C. Cascade-based attacks on complex networks. *Phys. Rev. E* **2002**, *66*, 065102. [CrossRef] [PubMed]
2. Crucitti, P.; Latora, V.; Marchiori, M.; Rapisarda, A. Efficiency of scale-free networks: Error and attack tolerance. *Phys. A Stat. Mech. Appl.* **2003**, *320*, 622–642. [CrossRef]
3. Wei, D.Q.; Luo, X.S.; Zhang, B. Analysis of cascading failure in complex power networks under the load local preferential redistribution rule. *Phys. A Stat. Mech. Appl.* **2012**, *391*, 2771–2777. [CrossRef]
4. Li, W.; Bashan, A.; Buldyrev, S.V.; Stanley, H.E.; Havlin, S. Cascading Failures in Interdependent Lattice Networks: The Critical Role of the Length of Dependency Links. *Phys. Rev. Lett.* **2012**, *108*, 228702. [CrossRef] [PubMed]
5. Yang, R.; Wang, W.-X.; Lai, Y.-C.; Chen, G. Optimal weighting scheme for suppressing cascades and traffic congestion in complex networks. *Phys. Rev. E* **2009**, *79*, 026112. [CrossRef] [PubMed]
6. Chang, L.; Wu, Z. Performance and reliability of electrical power grids under cascading failures. *Int. J. Electr. Power Energy Syst.* **2011**, *33*, 1410–1419. [CrossRef]
7. Wang, S.; Zhang, J.; Duan, N. Multiple perspective vulnerability analysis of the power network. *Phys. A Stat. Mech. Appl.* **2018**, *492*, 1581–1590. [CrossRef]
8. Wang, S.; Zhang, J.; Zhao, M.; Min, X. Vulnerability analysis and critical areas identification of the power systems under terrorist attacks. *Phys. A Stat. Mech. Appl.* **2017**, *473*, 156–165. [CrossRef]
9. Zhang, J.; Wang, S.; Wang, X. Comparison analysis on vulnerability of metro networks based on complex network. *Phys. A Stat. Mech. Appl.* **2018**, *496*, 72–78. [CrossRef]
10. Liu, H.; Tian, Z.; Huang, A.; Yang, Z. Analysis of vulnerabilities in maritime supply chains. *Reliab. Eng. Syst. Saf.* **2018**, *169*, 475–484. [CrossRef]
11. Zhang, J.; Xu, X.; Hong, L.; Wang, S.; Fei, Q. Attack vulnerability of self-organizing networks. *Saf. Sci.* **2012**, *50*, 443–447. [CrossRef]
12. Yi, C.; Bao, Y.; Jiang, J.; Xue, Y. Modeling cascading failures with the crisis of trust in social networks. *Phys. A Stat. Mech. Appl.* **2015**, *436*, 256–271. [CrossRef]

13. Zhao, Z.; Zhang, P.; Yang, H. Cascading failures in interconnected networks with dynamical redistribution of loads. *Phys. A Stat. Mech. Appl.* **2015**, *433*, 204–210. [CrossRef]
14. Buldyrev, S.V.; Parshani, R.; Paul, G.; Stanley, H.E.; Havlin, S. Catastrophic cascade of failures in interdependent networks. *Nature* **2010**, *464*, 1025–1028. [CrossRef]
15. Crucitti, P.; Latora, V.; Marchiori, M. A topological analysis of the Italian electric power grid. *Phys. A Stat. Mech. Appl.* **2004**, *338*, 92–97. [CrossRef]
16. Holme, P.; Kim, B.J.; Yoon, C.N.; Han, S.K. Attack vulnerability of complex networks. *Phys. Rev. E* **2002**, *65*, 056109. [CrossRef]
17. Allesina, S.; Pascual, M. Googling Food Webs: Can an Eigenvector Measure Species' Importance for Coextinctions? *PLoS Comput. Biol.* **2009**, *5*, e1000494. [CrossRef]
18. Qin, J.; Xu, J.J.; Hu, D.; Sageman, M.; Chen, H. Analyzing terrorist networks: A case study of the global salafi jihad network. *Lect. Notes Comput. Sci.* **2005**, *3495*, 287–304. [CrossRef]
19. Viljoen, N.M.; Joubert, J.W. The vulnerability of the global container shipping network to targeted link disruption. *Phys. A Stat. Mech. Appl.* **2016**, *462*, 396–409. [CrossRef]
20. Pu, C.-L.; Cui, W. Vulnerability of complex networks under path-based attacks. *Phys. A Stat. Mech. Appl.* **2015**, *419*, 622–629. [CrossRef]
21. Yingyi, H.; Chun, J. Model and analysis for cascading failure on logistics network based on local information of nodes. *Appl. Res. Comput.* **2013**, *9*, 2625–2628+2693. [CrossRef]
22. Huang, Y.Y.; Jin, C. Invulnerability analysis of logistics infrastructure network based on cascading failure. *Control Decis.* **2014**, *29*, 1711–1714. [CrossRef]
23. Jin, C.; Huang, Y.; Gao, P. Analysis on Cascading Failure Propagation in Logistics System under Emergency. In Proceedings of the 2010 International Conference on E-Product E-Service and E-Entertainment (ICEEE 2010), Henan, China, 7–9 November 2010; pp. 1–4.
24. Yong, L.I.; Jun, W.U.; Tan, Y.J. Invulnerability study for cascading failure of the logistics support networks of capacity evenly distributed. *J. Syst. Eng.* **2010**, *25*, 853–860.
25. He, X.; Yuan, Y.; Zhang, M. Node importance evaluation under cascading failure of logistics infrastructure coupled network. *Appl. Res. Comput.* **2018**, *7*, 20.
26. Zhang, G.S.; Liu, W. Mechanism of Network Vulnerability of Logistics Service Supply Chain Based on Complex Network Theory. *J. Bus. Econ.* **2016**, *12*, 19–27. [CrossRef]
27. Yan, Y.; Liu, X.; Zhuang, X.T. Cascading failure model and method of supply chain based on complex network. *Shanghai Jiaotong Daxue Xuebao/J. Shanghai Jiaotong Univ.* **2010**, *44*, 322–325,331.
28. Ducruet, C.; Ietri, D.; Rozenblat, C. Cities in Worldwide Air and Sea Flows: A multiple networks analysis. *Cybergeo Eur. J. Geogr.* **2011**, *528*. [CrossRef]
29. Kaluza, P.; Kölzsch, A.; Gastner, M.T.; Blasius, B. The complex network of global cargo ship movements. *J. R. Soc. Interface* **2010**, *7*, 1093–1103. [CrossRef]
30. Ducruet, C. Network diversity and maritime flows. *J. Transp. Geogr.* **2013**, *30*, 77–88. [CrossRef]
31. Tsiotas, D.; Polyzos, S. Effects in the network topology due to node aggregation: Empirical evidence from the domestic maritime transportation in Greece. *Phys. A Stat. Mech. Appl.* **2018**, *491*, 71–88. [CrossRef]
32. Cardillo, A.; Zanin, M.; Gómez-Gardeñes, J.; Romance, M.; del Amo, A.J.G.; Boccaletti, S. Modeling the multi-layer nature of the European Air Transport Network: Resilience and passengers re-scheduling under random failures. *Eur. Phys. J. Spéc. Top.* **2013**, *215*, 23–33. [CrossRef]
33. Joyez, C. On the topological structure of multinationals network. *Phys. A Stat. Mech. Appl.* **2017**, *473*, 578–588. [CrossRef]
34. Calatayud, A.; Mangan, J.; Palacin, R. Connectivity to international markets: A multi-layered network approach. *J. Transp. Geogr.* **2017**, *61*, 61–71. [CrossRef]
35. Vespignani, A. The fragility of interdependency. *Nature* **2010**, *464*, 984–985. [CrossRef]
36. Mahrukh, M.; Thomas, M.S. Load Altering Attacks—A Review of Impact and Mitigation Strategies. In Proceedings of the 2023 International Conference on Recent Advances in Electrical, Electronics & Digital Healthcare Technologies (REEDCON), New Delhi, India, 1–3 May 2023; pp. 397–402.
37. Wang, C.; Xia, Y.; Zhu, L. A method for identifying the important node in multi-layer logistic networks. *Front. Phys.* **2022**, *10*, 968645. [CrossRef]
38. Wang, J.-W.; Rong, L.-L. Cascade-based attack vulnerability on the US power grid. *Saf. Sci.* **2009**, *47*, 1332–1336. [CrossRef]
39. Wang, J.; Li, Y.; Zheng, Q. Cascading load model in interdependent networks with coupled strength. *Phys. A Stat. Mech. Appl.* **2015**, *430*, 242–253. [CrossRef]
40. Zhang, J.; Dai, Y.; Zou, K.; Song, B.; Zhang, Z. Vulnerability analysis of the US power grid based on local load-redistribution. *Saf. Sci.* **2015**, *80*, 156–162. [CrossRef]
41. Ducruet, C. Multilayer dynamics of complex spatial networks: The case of global maritime flows (1977–2008). *J. Transp. Geogr.* **2017**, *60*, 47–58. [CrossRef]
42. Duan, D.-L.; Ling, X.-D.; Wu, X.-Y.; OuYang, D.-H.; Zhong, B. Critical thresholds for scale-free networks against cascading failures. *Phys. A Stat. Mech. Appl.* **2014**, *416*, 252–258. [CrossRef]

43. Wang, J. Mitigation strategies on scale-free networks against cascading failures. *Phys. A Stat. Mech. Appl.* **2013**, *392*, 2257–2264. [CrossRef]
44. Zhao, L.; Park, K.; Lai, Y.-C. Attack vulnerability of scale-free networks due to cascading breakdown. *Phys. Rev. E Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.* **2004**, *70*, 035101. [CrossRef] [PubMed]
45. Halu, A.; Mukherjee, S.; Bianconi, G. Emergence of overlap in ensembles of spatial multiplexes and statistical mechanics of spatial interacting network ensembles. *Phys. Rev. E* **2014**, *89*, 012806. [CrossRef] [PubMed]
46. Li, P.; Wang, B.-H.; Sun, H.; Gao, P.; Zhou, T. A limited resource model of fault-tolerant capability against cascading failure of complex network. *Eur. Phys. J. B* **2008**, *62*, 101–104. [CrossRef]
47. Latora, V.; Marchiori, M. Efficient Behavior of Small-World Networks. *Phys. Rev. Lett.* **2001**, *87*, 198701. [CrossRef]
48. Barabási, A.-L.; Albert, R. Emergence of Scaling in Random Networks. *Science* **1999**, *286*, 509–512. [CrossRef]
49. Barrat, A.; Barthelemy, M.; Pastor-Satorras, R.; Vespignani, A. The architecture of complex weighted networks. *Proc. Natl. Acad. Sci. USA* **2004**, *101*, 3747–3752. [CrossRef]
50. Newman, M.E.J. The Structure and Function of Complex Networks. *SIAM Rev.* **2003**, *45*, 167–256. [CrossRef]
51. Watts, D.J.; Strogatz, S.H. Collective dynamics of 'small-world' networks. *Nature* **1998**, *393*, 440–442. [CrossRef]
52. Morone, F.; Makse, H.A. Influence maximization in complex networks through optimal percolation. *Nature* **2015**, *524*, 65–68. [CrossRef]
53. Newman, M.E. Scientific collaboration networks. I. Network construction and fundamental results. *Phys. Rev. E* **2001**, *64*, 016131. [CrossRef] [PubMed]
54. Taylor, P.J. Specification of the World City Network. *Geogr. Anal.* **2001**, *33*, 181–194. [CrossRef]
55. Xu, H.; Jin, F.; Wang, C. Optimization of the locations of hub-ports in round-the-world container service. *Dili Xuebao/Acta Geogr. Sin.* **2008**, *63*, 593–602.