systems

MDPI

Article

Vulnerability Analysis of the Sea–Railway Cross-Border Intermodal Logistics Network Considering Inter-Layer Transshipment Under Cascading Failures

Hairui Wei * and Huixin Qi

Business School, University of Shanghai for Science & Technology, Shanghai 200093, China; 232481141@st.usst.edu.cn

* Correspondence: hrwei@usst.edu.cn

Abstract

Maritime logistics and railway logistics are crucial in cross-border logistics, and their integration forms a sea-rail cross-border intermodal logistics network. Against the backdrop of frequent unexpected events in today's world, the normal operation of the sea-rail cross-border intermodal logistics network is under considerable threat. Therefore, researching the vulnerability of the intermodal network is extremely urgent. To this end, this paper first constructs a topological model of the sea-rail cross-border intermodal logistics network, designed to reflect the crucial process of "inter-layer transshipment" via transshipment nodes. Subsequently, a cascading failure model is developed to evaluate network vulnerability, featuring a load redistribution process that distinguishes between transshipment and non-transshipment nodes. The paper yields three primary findings. First, it identifies the optimal values for the capacity factor, overload factor, and inter-layer load transfer rate that most effectively mitigate the network's vulnerability. Second, compared to a single sub-network (such as a maritime logistics network or a railway logistics network), the sea-rail cross-border intermodal network exhibits lower vulnerability when facing attacks. Third, it highlights the critical role of transshipment nodes, confirming that their failure will make the entire sea-rail cross-border intermodal logistics network more vulnerable.

Keywords: cascading failure; inter-layer transshipment; maritime logistics; railway logistics; sea–railway cross-border intermodal logistics network; vulnerability

check for updates

Academic Editor: Emilio Larrodé

Received: 14 August 2025
Revised: 26 September 2025
Accepted: 8 October 2025
Published: 10 October 2025

Citation: Wei, H.; Qi, H. Vulnerability Analysis of the Sea–Railway Cross-Border Intermodal Logistics Network Considering Inter-Layer Transshipment Under Cascading Failures. *Systems* **2025**, *13*, 890. https://doi.org/10.3390/systems13100890

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Driven by the "Belt and Road" Initiative, cross-border logistics transport has developed rapidly and has become inseparable from the development of maritime logistics and railway logistics, two of its major pillars. While maritime logistics connect major trade ports around the world based on their large-scale ocean shipping capacity, cross-border railway logistics are responsible for efficiently handling cross-border and inland transport. In this context, the effective integration of maritime logistics networks and railway logistics networks gives rise to sea–railway cross-border intermodal logistics networks. This network enables the transfer of goods between rail and maritime logistics through the coordination of both logistics systems, overcoming the limitations of a single transport mode in dealing with complex international logistics demand.

Boccaletti et al. [1] proposed that a multilayer network can be viewed as a collection of multiple single-layer networks, where different single-layer networks are interconnected

through connections between nodes within the same layer and nodes in other layers, collectively forming the multilayer network. Drawing on this literature, the maritime logistics network and the railway logistics network are interconnected through transshipment nodes to jointly form the sea-rail cross-border intermodal logistics network model in this paper. These transfer nodes simultaneously function as both port terminals and railway transport hubs, serving as critical points for cargo flow. For example, Shanghai is not only a globally significant maritime hub but also possesses well-developed railway transport facilities, making it a critical transfer node connecting maritime logistics networks and railway logistics networks, thereby enabling smooth cargo transfer between the two networks. When a transfer node is disrupted, due to the occurrence of a chain reaction, it not only affects the normal operation of the network layer in which it resides but may also impact inter-layer logistics, thereby influencing the entire sea–railway cross-border intermodal logistics network. Therefore, for the sea–railway cross-border intermodal logistics network, its operation is influenced by both maritime and railway transportation modes.

The sea–railway cross-border intermodal logistics network is vulnerable to various "emergent events," including political conflicts (such as wars or terrorist attacks), natural disasters (such as earthquakes, floods, etc.), and human errors (such as operational mistakes or technical malfunctions). In this network, the failure of a single node can lead to cascading failures, resulting in widespread system breakdowns across the entire network. For instance, in 2024, the Red Sea crisis disrupted this critical maritime route for global trade, forcing a large volume of time-sensitive cargo to shift to China-Europe Railway Express services [2]. Similar examples include the severe damage caused by Hurricane Sandy to the Port of New York, surrounding ports, railway systems, and related supply chains in 2012 [3], as well as the 2021 incident where the grounding of the Ever Given due to human error resulted in the blockage of the Suez Canal—the most critical waterway between Europe and Asia—exerting a significant impact on global trade and supply chains [4]. Against this backdrop, it is of great necessity to study the vulnerability of the cross-border sea-rail intermodal logistics network.

In traditional studies on the vulnerability of transportation and logistics networks, research has primarily focused on the vulnerability of single-modal, single-layer network models [5–7]. In the cross-border sea-rail intermodal logistics network, traditional topological models fail to characterize the ability of cargo to transfer between railway and maritime logistics networks via these transshipment nodes, thereby enabling "inter-layer transshipment." Such "inter-layer transshipment" cannot be captured by conventional topological models. Therefore, to more accurately reflect the actual operational conditions of the cross-border sea-rail intermodal logistics network, it is essential to incorporate the transshipment characteristics between maritime and railway logistics into the construction of research models. However, studies on the vulnerability of sea–railway cross-border intermodal logistics networks that incorporate this critical transshipment mechanism are still considerably lacking.

Therefore, this paper focuses on the vulnerability of the sea–railway cross-border intermodal logistics network considering inter-layer transshipment. The main research problems of this paper are as follows: first, how to construct a topological model of a sea–railway cross-border intermodal logistics network that can reflect the transshipment process; second, how to incorporate the phenomenon of inter-layer transshipment into a cascading failure model in order to more accurately assess the vulnerability of the sea–railway cross-border intermodal logistics network.

The research approach and framework proposed in this paper are illustrated in Figure 1. This paper begins with the formulation of the research questions, followed by the construction of a topological model of the sea–railway cross-border intermodal

logistics network that reflects the transshipment process. Next, based on the classical ML capacity-load model, this paper improves and optimizes the model by incorporating the characteristics of the sea–railway cross-border intermodal logistics network, thereby designing a cascading failure mechanism, includes reasonably setting node capacities and initial loads, establishing clear node state determination mechanisms to ensure the model accurately reflects the actual network operation, and proposing a new load redistribution strategy to address the differences between transshipment and non-transshipment nodes in load redistribution. Building on this, this paper analyzes the vulnerability of the sea–railway cross-border intermodal logistics network under different attack modes and parameter settings through simulation experiments. Finally, conclusions are drawn and summarized.

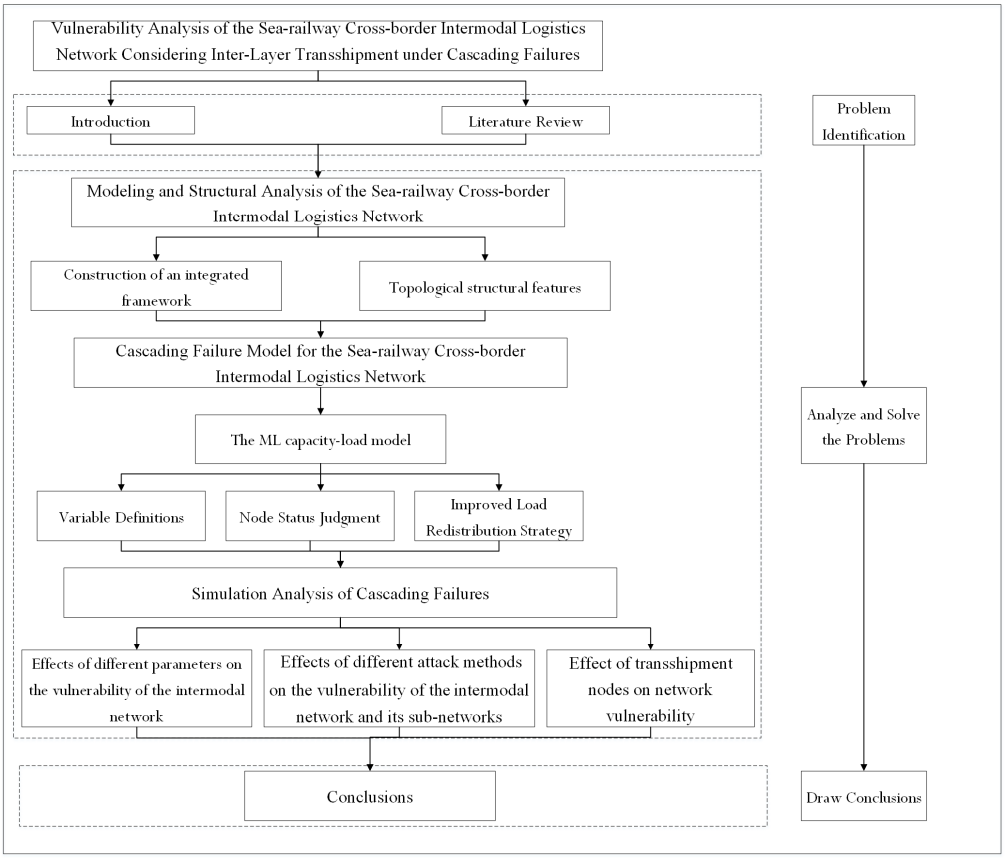

Figure 1. The structure of the paper.

The remainder of this paper is organized as follows: Section 2 reviews the literature related to the research content of this paper. In Section 3, a sea–railway cross-border intermodal logistics network is constructed, and its topological structure is evaluated. Section 4 describes the modeling of a cascading failure model considering inter-layer transshipment, and the simulation results are simulated and analyzed in Section 5. Section 6 draws the conclusions and provides several suggestions.

2. Literature Review

Currently, there is a rich body of research on the vulnerability of transportation and logistics networks. This paper will conduct a literature review from two dimensions: research questions and research methods. Firstly, it will analyze the research progress on the vulnerability of transportation and logistics networks and then sort out the methods for studying this issue, so as to provide theoretical references and methodological support for subsequent research.

2.1. Vulnerability of Traffic and Logistics Networks

In recent years, global transportation and logistics networks have frequently faced disruptions caused by natural disasters [8,9], political conflicts [10], and human factors [4,11]. These cases have fully exposed the vulnerability of transportation and logistics networks when confronted with such disruptions, thereby prompting academic research in this field.

Jiang et al. [12] examined the vulnerability of maritime supply chain networks. Guo et al. [13] constructed an "irreplaceability" model based on the geographical locations of ports to conduct a vulnerability simulation analysis of shipping networks under the impact of emergencies. Tao et al. [14] characterized the impact of node failures on the vulnerability of maritime logistics networks by integrating normalized centrality scores and multi-scale factors and validated the model's effectiveness using the Asia-Europe maritime transportation network as a case study. Zhou et al. [15] proposed a new network efficiency index—Layered Weighted Network Efficiency (LWNE)—to evaluate the vulnerability characteristics of air transportation networks under disruptions at different layers. Wu et al. [16] explored the method of identifying the critical point of collapse of container shipping networks under a deliberate attack and quantitatively analyzed the variation trend of network vulnerability. It can be observed that the aforementioned studies primarily focus on single-layer networks, neglecting the vulnerability of intermodal transportation networks. However, in actual transportation systems, various types of networks typically do not exist in isolation; instead, they operate collectively through multiple modes of transportation. Therefore, single-layer networks can hardly reflect the complex relationships between different networks.

With the advancement of research, scholars have gradually shifted their focus to multi-layer networks [17,18]. Most scholars have focused on assessing the overall vulnerability of multi-layer networks. Numerous scholars have specifically investigated the vulnerability of sea–land intermodal networks. For instance, Zhang et al. [19] chose the sea–railway cross-border intermodal logistics network composed of the China Railway Express and sea lane data as the research object and studied its vulnerability. Zhang et al. [20] constructed a bilayer China-Europe sea–railway transport network model based on the supra-adjacency matrix and conducted an analysis by simulating the factors affecting network vulnerability, as well as its variation patterns. Xiong et al. [21] investigated the interactive propagation mechanisms of risks and failures within the sea-rail intermodal network under the Belt and Road Initiative, while also incorporating recovery mechanisms into their analysis. Lu et al. [22] proposed a cascading failure model for the seaport-dry port network in container transportation, and based on this, analyzed the network's resilience. Feng et al. [23] developed a composite transport network for the New Western Land–Sea Corridor, which integrates road, rail, and sea freight, and evaluated its vulnerability to cascading failures. Additionally, some scholars have investigated the vulnerability of intermodal networks formed by integrating other modes of transport. For example, Wang et al. [24] evaluated the vulnerability of the Chinese Coupled Aviation and High-Speed Railway network from the perspective of ground transfer interruption and explored the variations in its vulnerability under different failure time intervals. Ferrari et al. [25] analyzed the vulnerability of an intermodal network, composed of highways and railways, in emergency situations. Ippolito et al. [26] evaluated the robustness of the multi-layer network integrated by the European aviation network and railway network and quantitatively analyzed the importance of nodes within it. Although Boura et al. [27] mentioned that discrete transportation infrastructure networks (such as highways and railways) have geographical interdependencies, they did not delve into the transshipment mechanisms between different transportation networks. Clearly, scholars have begun to pay attention to multi-layer networks that can better describe the charac-

teristics of real networks. However, current studies tend to overlook the impact of nodes with transshipment functions on network vulnerability. These nodes can transfer goods to different transportation networks through inter-layer transshipment and are therefore crucial to the operation of the overall intermodal network.

In summary, building upon existing research, this paper further advances the field by constructing a sea–railway cross-border intermodal logistics network model, breaking through the limitations of traditional single-transportation network modeling. Secondly, different from most existing multi-layer transportation network modeling, this paper takes into account the characteristic that transshipment nodes in the cross-border sea-rail intermodal logistics network connect maritime logistics networks and railway logistics networks and constructs an intermodal network model that can describe transshipment characteristics to evaluate its vulnerability. Additionally, it separately studies the impact of transshipment nodes on the vulnerability of the intermodal network. The network model constructed in this paper is more applicable to today's complex transportation and logistics networks, broadening the research perspective on intermodal networks.

2.2. Overview of Research Methods

The analysis methods for the vulnerability of transportation networks are relatively diverse. The vulnerability analysis of transportation and logistics networks mainly involves two aspects: first, identifying key nodes in the network based on network eigenvalues [28]; second, removing nodes on the basis of evaluating node importance, conducting simulations to predict the impact of node failures on the operational stability of the network, and using changes in a series of indicators as quantitative metrics to evaluate vulnerability, such as degree, average shortest path length, clustering coefficient, and global network efficiency [29–32]. Currently, the academic community has generally focused on the impact of cascading failures on the vulnerability of complex networks [33–35]. Cascading failure refers to a phenomenon where the failure of one node in a network causes subsequent failures of other nodes, ultimately leading to a significant decline or complete collapse of the entire network's functionality [36]. Existing cascading failure models mainly include the coupled map lattices model [37–40], the capacity-load model [41–43], the binary effect model [44], and the disaster propagation model [45]. Among them, the capacity-load model is the most widely used model, the key to which lies in its load redistribution strategies [46]. Regarding research on load redistribution strategies, some scholars do not distinguish between node characteristics and allocate loads based on uniform rules, such as the average allocation strategy [47]. Some other scholars have designed strategies tailored to node differences, including allocation based on node degree [48], allocation based on node capacity [49], etc. In addition, Wang et al. [50] examined the influence of airport categories on load redistribution and developed a strategy based on airport grades. Liang et al. [51] proposed a strategy that considers the real-time processing capacity of nodes for load redistribution. Lu et al. [52] introduced a load redistribution method based on port cooperation mechanisms and found that such cooperation mechanisms can significantly mitigate the losses incurred by shippers due to port failures. Cumelles et al. [53] pointed out that in the cascading failures of airport networks, loads need to be redistributed among adjacent airports rather than via existing connections. It can be observed that the academic community has conducted various explorations and improvements in load redistribution strategies. However, research on load redistribution strategies designed for the functional differences in nodes in intermodal transportation networks remains insufficient.

For the sea–railway cross-border intermodal logistics network proposed in this paper, cities where transshipment nodes are located have two modes of transport, namely, sea transport and railway transport. They bear important transshipment functions, making it

possible to transfer cargoes between different network layers via these transshipment nodes. While this characteristic of transshipment nodes establishes the existence of differences between transshipment nodes and other nodes in the process of load redistribution, it is rarely touched upon in the existing literature. Based on this, this paper improves the load redistribution strategy on the basis of the traditional cascading failure model and proposes a cascading failure model that considers the differences in load redistribution between transshipment nodes and non-transshipment nodes to analyze the cascading failure process of the sea–railway cross-border intermodal logistics network. This enriches the existing capacity-load model and provides new methodological support for the research on cascading failures in intermodal transportation networks.

3. Modeling and Structural Analysis of the Sea–Railway Cross-Border Intermodal Logistics Network

Constructing a network model and analyzing its structural characteristics serves as the prerequisite for subsequent research on network vulnerability. Based on actual data along the "Belt and Road," this paper constructs a sea–railway cross-border intermodal logistics network model and applies complex network knowledge to analyze the network's topological structure, thereby laying the foundation for subsequent vulnerability research.

3.1. Construction of an Integrated Framework

The sea–railway cross-border intermodal logistics network is a two-layer network, with one layer representing the maritime sub-network and the other representing the railway sub-network. The two layers are connected through inter-layer links between the transshipment nodes. In network modeling, a seaport and a railway station located within the same city as transshipment nodes in the maritime and railway sub-networks, respectively. These two nodes are connected by an inter-layer link, which facilitates the "inter-layer transshipment" of goods between the maritime and railway layers. Figure 2 presents the structural schematic of the sea–rail cross-border intermodal logistics network.

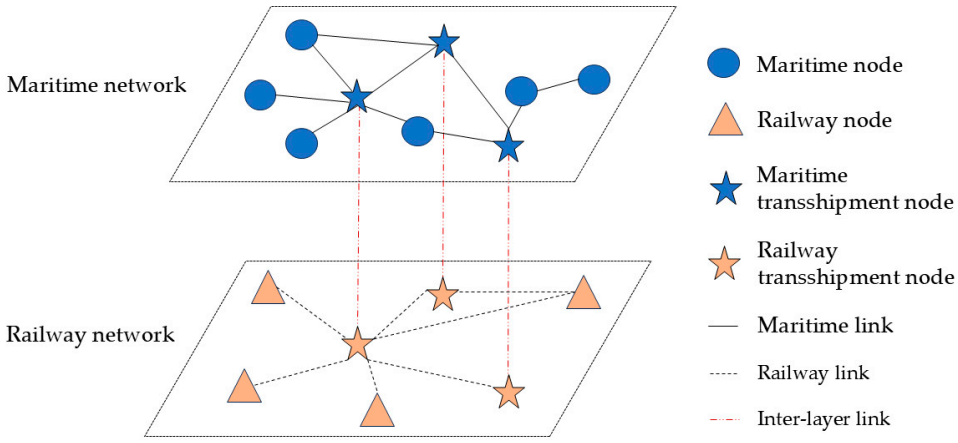

Figure 2. Sea–railway cross-border intermodal logistics network.

Considering that the Belt and Road Initiative covers a multitude of countries and regions, with its transportation network integrating two core modes of transport—maritime shipping and railway—it constitutes an important component of the international logistics network system. Therefore, this paper constructs a sea-rail cross-border intermodal logistics network using data that link the ports and railway terminals along the Belt and Road Initiative route. The data sources of the network model are as follows. The route data of the maritime network are derived from the shipping schedules of the top 10 container liner companies in the world (ranked by shipping capacity), provided by Alphaliner. The nodes

of the maritime network include the major ports of these shipping companies. The nodes of the railway network comprise major railway freight hub cities in Central Asia, Central Europe, and along the China–Southeast Asia routes, with the fundamental routes primarily derived from official sources such as the China-Europe Railway Express website. These data are then used to construct a sea–railway cross-border intermodal logistics network composed of 308 nodes and 1378 edges. Specifically, the maritime network consists of 214 nodes and 1020 edges, while the railway network consists of 94 nodes and 336 edges. There are 44 transshipment nodes with inter-layer transshipment functions.

Since the focus of this study is on the impact of cascading failures on network structure, and to simplify the analysis, the storage, processing time, and additional costs associated with the inter-layer transshipment in real-world scenarios are ignored. The goods are abstracted as standardized load units. The modeling of "inter-layer transshipment" in this paper is a simplified description of the logistics process, rather than a simulation of the actual transshipment process. In this network, cargos can be transported bidirectionally along the network structure. That is, this network supports both the bidirectional circulation of cargos along the intra-layer transport route in each sub-network and the inter-layer transfer of cargos between the maritime network layer and the railway network layer via transshipment nodes.

3.2. Topological Structural Features

The existing literature has identified the maritime network as a complex network [54]. Based on the structural analysis indicators of complex networks (see Table 1 [55] for details), this study uses the complex network analysis software Ucinet 6 to calculate and analyze the constructed intermodal network, and the obtained structural indicator values are presented in Table 2.

Table 1. Meanings of topological indicators.

Topological Indicator	Meaning
Degree	The number of other nodes directly connected to the node in the network
Degree distribution	Degree dispersion of nodes
Average degree	The average of the degrees of all nodes in the network
Cluster coefficient	The degree to which nodes form triangles (i.e., interconnected triples) in the network
Path length	The number of edges passed by the shortest path from one node to another in the network
Average path length	The average of the shortest path lengths between all node pairs in the network

Table 2. Topological indicator values.

Network Type	Average Degree	Cluster Coefficient	Average Path Length
Intermodal network	8.9481	0.3322	3.3904
Maritime network	9.5327	0.4041	2.9289
Railway network	7.1489	0.2074	2.3015

The degree of a node refers to the number of other nodes directly connected to the node in the network. As shown in Table 2, the average degree value of the maritime network is larger than that of the railway network, and the intermodal network falls between them in this regard. Using the curve fitting function in MATLAB, the probability distribution curve of nodes in the intermodal network is obtained as shown in Figure 3. Function fitting shows that, compared with the general power-law distribution function, the truncated power-law distribution function has a higher goodness-of-fit. Overall, the degree distribution of nodes in the intermodal network conforms to the functional form of $y = 0.16\hat{}0.28e\hat{}(-0.22x)$, where the square sum of the error (SSE) is 0.0055, which is close

to zero. This result indicates that the difference between predicted and observed values is small. The coefficient of determination (R^2) is 0.9178, implying that the model has a strong ability to explain data variations and a high goodness-of-fit of the data. This result testifies to the scale-free property of the intermodal network. That is, the nodes with large degree values account for a small proportion in the network, while those with small degree values account for a large proportion.

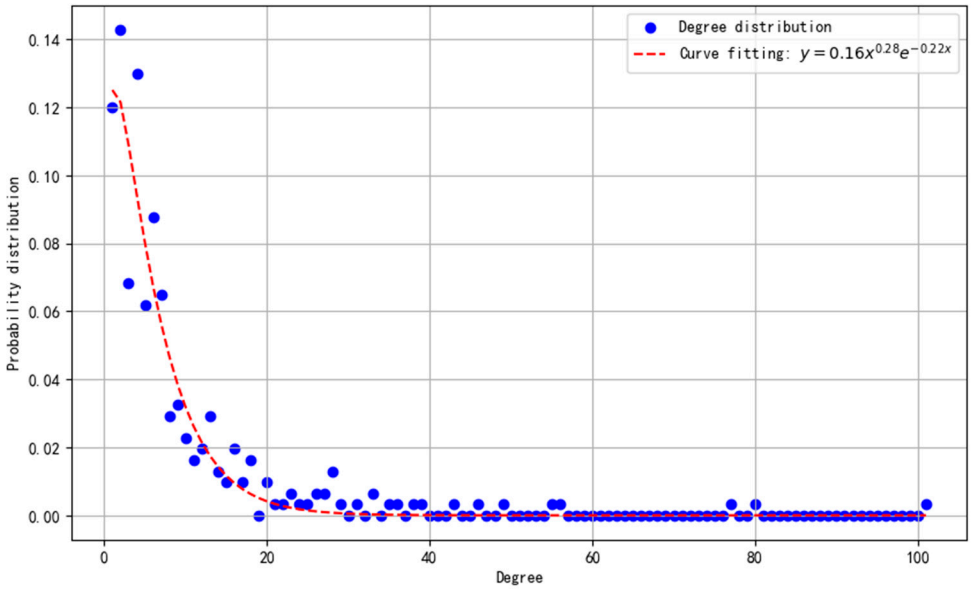

Figure 3. Degree distribution and fitting curve of the intermodal network.

The scale-free characteristic of the intermodal network indicates that a small number of nodes (such as key ports and railway hub cities) are connected to the majority of other cities. This characteristic causes the intermodal network to exhibit different vulnerabilities when facing random or deliberate attacks. Therefore, based on an analysis of the topological characteristics of the intermodal network, this paper explores how cascading failures under deliberate and random attacks affect the vulnerability of the sea–railway intermodal network.

The cluster coefficient reflects the closeness of interconnection between nodes in the network. According to Table 2, the cluster coefficient of the maritime network is larger than that of the railway network, and the intermodal network ranges between them in this regard. Although the intermodal network has the largest average path length, the cargos in it may need to be transshipped multiple times between maritime and railway networks; therefore, its cargo transport efficiency is lower than that of each single-layer network. Nevertheless, when an ER-random network with the same scale as the intermodal network is constructed, i.e., when its number of nodes is set to 308, its average path length is 2.8738 (which is close to the average path length of 3.3904 of the intermodal network), and its cluster coefficient is 0.0270. The cluster coefficient of the intermodal network is significantly larger than that of the random network. This result suggests that the intermodal network, which is characterized by a large cluster coefficient and a small average path length, is a small-world network [56].

In summary, the intermodal network is a complex network characterized by scale-free and small-world properties. In the follow-up analysis, a series of complex network theories and methods are combined with the cascading failure model to further analyze the vulnerability of the sea–railway cross-border intermodal logistics network.

4. Cascading Failure Model for the Sea–Railway Cross-Border Intermodal Logistics Network

It should be specifically noted that this paper focuses on the impact of node (port, railway station) failures on the sea-rail cross-border intermodal network and does not consider the interruption of edges (railway lines, maritime shipping segments). In this context, a cascading failure refers to the phenomenon that, after a node fails in a network, the impact of this failure gradually propagates to other parts of the network, ultimately triggering the partial or complete functional failure of the entire network [57]. In a sea–railway cross-border intermodal logistics network, when a node fails because of a natural disaster or human sabotage, because of the interconnection between nodes, this failure may propagate within the network where the failed node is located, or even to other networks. If no measure is taken, the failure may ripple across the entire intermodal network, resulting in a considerable loss of network functionality.

The classic Motter–Lai cascade model [58] is widely used in cascading failure research. This model assumes that each node has an initial load L_i, and the node capacity C_i has a linear relationship with the initial load, i.e., $C_i = L_i + \alpha L_i$, where α is the capacity coefficient. When a node j in the network fails, its load L_i will be redistributed to adjacent nodes i, and the transferred load is denoted as ΔL_{ji}. At this point, the load of node i increases to $L_i + \Delta L_{ji}$. If the load of node i thus exceeds its capacity, node i will also fail, further affecting the functionality and stability of the entire network. Building on the classic Motter–Lai cascade model, this paper improves and optimizes the model in combination with the characteristics of the research problem. Compared with the traditional capacity-load model, the cascading failure model constructed in this paper has differences in several aspects:

(1) There are overloaded loads. In the classical model, each node is in either of two states, optimal or failed. However, in the actual operation of a sea–railway cross-border intermodal logistics network, as each node can withstand overloading to some extent, the load of a node may exceed its capacity within a certain range, that is, it may function in an overloaded state.

(2) The transition of a node from overloaded to a failed state is probabilistic. In the traditional ML model, once a node is overloaded, its state will immediately change from "optimal" to "failed". In this paper, the bearing capacity of nodes in the overloaded state is considered. That is, when a node is overloaded, it does not fail immediately but fails according to a certain probability. This design can more truthfully reflect the actual network situation.

(3) The differences between transshipment nodes and non-transshipment nodes in terms of load redistribution are considered. In existing load redistribution strategies, the differences between nodes with transshipment functions and non-transshipment nodes are often ignored. In reality, for a node with transshipment functions, its load is not only transferred within the sub-network to which it belongs but also shifted by a certain proportion to another sub-network via inter-layer links.

4.1. Capacity and Initial Load

The initial load of a node refers to the volume of traffic borne by it at the beginning of network operation. Considering the features of nodes in the sea–railway cross-border intermodal logistics network, in this paper, the initial load of a node is defined as the actual freight volume of the ports or railways passing through the node, expressed as L_i (unit: TEU).

The capacity of a node, having an optimal value, refers to the maximum load the node can continuously process under the premise of maintaining both optimal performance

and stable operation. Exceeding this value may cause node congestion and lower work efficiency. Assuming that there is a linear relationship between the optimal capacity and initial load of a node, this paper defines the optimal capacity of a node as [43]:

$$C_i = L_i + \alpha \cdot L_i \tag{1}$$

where α denotes the capacity coefficient, used to adjust the optimal capacity of a node, representing the additional load capacity a node can withstand beyond handling the initial load, and $\alpha > 0$.

As the maximum load that can be handled by a node is limited by factors such as the sizes of ports and railway sites and the quantity of equipment, there is an upper limit of processing capacity for each node. It is assumed that the maximum capacity of a node follows a linear relationship with its optimal capacity:

$$C_{i(max)} = \theta \cdot C_i \tag{2}$$

where $C_{i(max)}$ denotes the maximum capacity of the node; θ denotes the overload factor, which reflects the additional load capacity a node can withstand when exceeding its optimal capacity.

4.2. Judging the Node State

After the node i receives the load distributed from neighboring nodes at t, if the load of the node at this point is less than its optimal capacity, the node will be in an optimal state. In contrast, if the load of the node at this point is greater than the upper limit of its processing capacity, the node will fail. Notably, if at this point, the load of the node is greater than its optimal capacity but less than the upper limit of its processing capacity, the node will fail at a certain probability or will be overloaded. Therefore, the state of a node, "optimal, overloaded, or failed", is mainly determined by the size of the load received by the node [59]:

$$S_i = \begin{cases} S_{optimal} & , L_i(t) \le C_i \\ S_{congesion} & , C_i < L_i(t) \le \theta C_i, \delta_i > P_i \\ S_{invalid} & , C_i < L_i(t) \le \theta C_i, \delta_i \le P_i \\ S_{invalid} & , L_i(t) > \theta C_i \end{cases} \tag{3}$$

where S_i denotes the state of node i; δ denotes a randomly generated number between 0 and 1, reflecting random disturbances that affect the stability of nodes in real-world logistics, such as transportation delays or equipment failures, and other uncertainties; P_i denotes the failure probability of node i, representing the likelihood of node i failing within a certain period of time.

When a node is in the optimal state, it can receive new load transferred from neighbor nodes. However, when it is in the overloaded or failed state, it will only distribute its load to nodes in the optimal state, instead of receiving new load. The overload capacity and redundancy capacity of a node enhance its load-bearing capacity, so that it, instead of failing immediately when the load exceeds the capacity, will fail according to a certain probability. In this case, the failure probability obeys an exponential distribution, where P_i can be expressed as follows [59]:

$$P_i = \begin{cases} 0 & , S_i = S_{optimal} \\ \frac{1}{1 - exp\left(-\frac{L_i - C_i}{(\theta - 1) \cdot C_i}\right)} & , S_i = S_{congesion} \cap \delta_i > P_i \\ 1 & , S_i = S_{invalid} \end{cases} \tag{4}$$

Among them, when node i is in an optimal state, its failure probability P_i is 0, indicating that the node has not failed. When the node enters an overload state and δ exceeds the current failure probability, the node's failure probability follows an exponential distribution. Once the node fails, its failure probability P_i becomes 1.

4.3. Load Redistribution Strategies

The strategy of redistributing the load of an overloaded or failed node in the network to other optimal nodes is called the load redistribution strategy. The sea–railway cross-border intermodal logistics network is a bilayer network composed of maritime and railway networks via transshipment nodes. This means that, when a node with transshipment functions is overloaded or fails, its load is not only transferred within the sub-network to which it belongs, but also shifted by a certain proportion to another sub-network via inter-layer links. Therefore, this paper proposes a load redistribution strategy considering inter-layer transshipment, which divides nodes into transshipment nodes and non-transshipment nodes, thereby distinguishing between them in terms of load redistribution. This division is more in line with the features of the sea–railway cross-border intermodal logistics network. When the load of a node is redistributed, nodes with closer connections with the node tend to receive a higher load. That is, it is easier for the load to be transferred between nodes with greater logistics attractiveness. Accordingly, this paper puts forward a load redistribution strategy based on the logistics attractiveness between nodes.

4.3.1. Modified Logistics Attractiveness Model Considering Node Importance

For a logistics physical network, the distance between nodes and the importance of nodes in the entire network are often important factors affecting the closeness between nodes [60,61]. Therefore, considering the distance between nodes and the importance of nodes in the entire network, in this paper, the following modified logistics attractiveness model is constructed based on the traditional logistics attractiveness model, to evaluate the logistics attractiveness between nodes. The formula is as follows:

$$F_{ij} = k \cdot \frac{I_i \cdot I_j}{D_{ij}^{\gamma}} \tag{5}$$

where nodes i and j are neighbor nodes; F_{ij} denotes the logistics attractiveness between them; k denotes the attractiveness coefficient, often set at 1; D_{ij} denotes the actual distance between nodes i and j; γ denotes the distance attenuation coefficient, typically set to 2 [62]; I_i and I_j denote the importance of node i and that of node j in the sea–railway cross-border intermodal logistics network, respectively.

Considering the physical network features of sea–railway intermodal networks, it can be concluded that multiple factors affect the importance of nodes in a network [63]. It is necessary to not only examine the evaluation indicators for node importance in traditional complex networks, such as the "centrality" indicator, which refers to the degree to which an individual (or participant) occupies a central position in the network [64]. This study selects four centrality indicators: degree centrality, closeness centrality, betweenness centrality, and eigenvector centrality [55]. Meanwhile, considering the physical characteristics of the sea-rail cross-border intermodal logistics network—specifically, that the logistics network is not merely a topological structure but also undertakes specific cargo flow functions—this paper also selects the freight volume passing through the node (in 10,000 TEU) as an indicator. Topological structural features and physical network features are organically combined to evaluate the importance of nodes in the network. The specific indicators are introduced as follows:

(1) Degree centrality is used to measure the importance or influence of a node in a network. In a complex network, the degree of a node refers to the number of edges directly connected with the node. This basically means that nodes with a higher degree centrality have greater importance.

$$C_D(i) = \frac{D(i)}{N-1} \tag{6}$$

where $C_D(i)$ denotes the degree centrality of node i, $D(i)$ denotes the degree of node i, and N denotes the total number of nodes in the network.

(2) Closeness centrality is usually defined as the reciprocal of the sum of the shortest path distances from a node to all other nodes in the network. Normalized closeness centrality can be expressed as:

$$C_C(i) = \frac{N-1}{\sum_{i \neq j} d(i,j)} \tag{7}$$

where $C_C(i)$ denotes the closeness centrality indicator of node i, and $d(i,j)$ denotes the shortest path length from node i to node j.

(3) Betweenness centrality is defined as the frequency at which a node falls on the shortest paths between pairs of other nodes in the network. Normalized betweenness centrality can be expressed as:

$$C_B(i) = \frac{2 \cdot \sum_{\substack{j,l \\ j \neq l \neq i}} \left[N_{jl}(i) / N_{jl} \right]}{(N-2) \cdot (N-1)} \tag{8}$$

where $C_B(i)$ denotes the betweenness centrality indicator of node i, N_{jl} denotes the total number of shortest paths between node j and node l, and $N_{jl}(i)$ denotes the total number of shortest paths by which node j and node l pass through node i.

(4) Eigenvector centrality emphasizes that node importance is related to both the node's own network position and the quantity and quality of its neighboring nodes. All nodes can be represented by an adjacency matrix M. When two nodes are connected, the corresponding element m_{ij} in the adjacency matrix is denoted as 1; otherwise, it is 0. The eigenvector centrality can then be expressed as follows:

$$C_E(i) = q \sum_{j=1}^{n} m_{ij} C_E(i) \tag{9}$$

where $C_E(i)$ represents the eigenvector centrality index of node i; the constant q is the reciprocal of the largest eigenvalue in the adjacency matrix M.

(5) In a sea–railway cross-border intermodal logistics network, nodes that can handle more cargos often enjoy higher status and greater influence in the network. In this paper, freight volume refers to the actual freight volume of ports or railways passing through the node, or the city where the node is located (unit: 10,000 TEU).

The above node importance evaluation indicator system implies that each indicator represents one aspect of importance. To objectively reflect the objective impact of each index value on node importance, this paper employs the TOPSIS-entropy weight method to evaluate the importance of nodes in the sea-rail cross-border intermodal logistics network [65]. The specific process is described as follows:

① Assuming that there are n nodes and m evaluation indicators in the network and that the jth indicator of the ith node can be expressed as x_{ij}, then the following decision matrix can be constructed:

$$A = (x_{ij})_{n\times m} = \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1m} \\ x_{21} & x_{22} & \dots & x_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \dots & x_{nm} \end{bmatrix} \tag{10}$$

② By standardizing the matrix to eliminate the effects of different dimensions on the results, the standardized matrix Z is obtained. The standardization formula for each element in Z is as follows:

$$Z_{ij} = x_{ij} / \sqrt{\sum_{i=1}^{n} x_{ij}^2} \tag{11}$$

③ Next, the proportion of the value of the ith node in the jth indicator, W_{ij}, can be calculated as follows:

$$W_{ij} = Z_{ij} / \sum_{i=1}^{n} Z_{ij}, (j = 1,\ 2\ ,\ \dots,\ m) \tag{12}$$

The entropy R_j of the jth indicator is as follows:

$$R_j = -\frac{1}{ln\ n} \cdot \sum_{i=1}^{n} W_{ij} \cdot ln\ W_{ij},\ (j = 1,\ 2,\ \dots,\ m) \tag{13}$$

④ The difference coefficient G_j of the jth indicator is:

$$G_j = 1 - R_j \tag{14}$$

The weight H_j of the jth indicator is as follows:

$$H_j = \frac{G_j}{\sum_{j=1}^{m} G_j} \tag{15}$$

⑤ Then, positive and negative ideal solutions are determined as follows:

$$\begin{gathered} Z^+ = (Z_1^+,\ Z_2^+,\ \dots,\ Z_m^+) \\ = (max\{z_{11},\ z_{21},\ \dots,\ z_{n1}\},\ max\{z_{12},\ z_{22},\ \dots,\ z_{n2}\},\ \dots,\ max\{z_{1m},\ z_{2m},\ \dots,\ z_{nm}\}) \end{gathered} \tag{16}$$

$$\begin{gathered} Z^- = (Z_1^-,\ Z_2^-,\ \dots,\ Z_m^-) \\ = (min\{z_{11},\ z_{21},\ \dots,\ z_{n1}\}, min\{z_{12},\ z_{22}, \dots,\ z_{n2}\}, \dots,\ min\{z_{1m},\ z_{2m},\ \dots,\ z_{nm}\}) \end{gathered} \tag{17}$$

The distances from the node to these positive and negative optimal solutions can be calculated using the Euclidean distance via the following formulae:

$$d_i^+ = \sqrt{\sum_{j=1}^{m} \left(Z_j^+ - z_{ij}\right)^2} \tag{18}$$

$$d_i^- = \sqrt{\sum_{j=1}^{m} \left(Z_j^- - z_{ij}\right)^2} \tag{19}$$

⑥ The degree of closeness to an optimal solution can be calculated via the following formula:

$$I_i = \frac{d_i^+}{d_i^+ + d_i^-} \tag{20}$$

Here, the degree of closeness to an optimal solution obtained is the importance score of the node in the sea–railway cross-border intermodal logistics network.

4.3.2. Loads of Transshipment Nodes and Non-Transshipment Nodes

When a transshipment node is overloaded, the portion of its load that exceeds the optimal capacity will be redistributed to other nodes. When a transshipment node fails, its load will be redistributed entirely. Accordingly, a load redistribution formula considering node state and inter-layer transfer can be given below:

① Inter-layer transfer of load from a transshipment node:

When the overloaded node is a transshipment node, a portion of its load is transferred to another sub-network via inter-layer links. The following are load redistribution formulae for the inter-layer transfer of the load when the transshipment node is overloaded and when it fails:

$$\Delta L_{(i\to j)} = \pi\cdot(L_i(t) - C_i) \tag{21}$$

$$\Delta L_{(i\to j)} = \pi\cdot L_i(t) \tag{22}$$

where i and j denote transshipment nodes with different transport functions (sea transport and railway transport) in the same city, respectively. They are located in different network layers and connected via inter-layer links. $\Delta L_{(i\to j)}$ denotes the load transferred from node i to node j; π denotes the inter-layer transfer rate of load, defined as the proportion (π) of load transferred via inter-layer links from the network layer where node i is located to the network layer where node j is located.

② Intra-layer transfer of load from a transshipment node:

When the overloaded node is a transshipment node, in addition to the inter-layer transfer of load, there is also the redistribution of the remaining portion of load in the sub-network where it is located according to the attractiveness model between nodes. The following are the load redistribution formulae for the intra-layer transfer of load when the transshipment node is overloaded (Equation (23)) and fails (Equation (24)):

$$\Delta L_{i_1\to i_2} = (1-\ \pi)\cdot(L_{i1}(t) - C_{i1})\cdot\frac{F_{i_1 i_2}}{\sum_{o\in N_{i1}^{neighbor}}^{o} F_{i1o}} \tag{23}$$

$$\Delta L_{i_1\to i_2} = (1-\pi)\cdot L_{i1}(t)\cdot\frac{F_{i_1 i_2}}{\sum_{o\in N_{i1}^{neighbor}}^{o} F_{i1o}} \tag{24}$$

where i_1 denotes a transshipment node; i_2 denotes a neighbor node of i_1, located in the same sub-network as i_1; $\Delta L_{i_1\to i_2}$ denotes the load transferred from node i_1 to node i_2; $(1-\ \pi)$ denotes the proportion ($(1-\ \pi)$) of load transferred within the layer; $F_{i_1 i_2}$ denotes the attractiveness between node i_1 and node i_2; $\sum_{o\in N_{i_1}^{neighbor}}^{o} F_{i_1 o}$ denotes the sum of the attractiveness between node i_1 and all its neighbor nodes.

The rules governing the load redistribution of non-transshipment nodes according to the node state are consistent with those governing the load redistribution of transshipment nodes, except that the load of a non-transshipment node is only transferred within the layer in the sub-network where it is located according to the attractiveness model between nodes.

The following are the load redistribution formulae for the intra-layer transfer of load when the non-transshipment node is overloaded (Equation (25)) and when it fails (Equation (26)):

$$\Delta L_{i_3 \to i_4} = \left(L_{i_3}(t) - C_{i_3}\right) \cdot \frac{F_{i_3 i_4}}{\sum_{o \in N_{i_3}^{neighbor}}^{o} F_{i_3 o}} \tag{25}$$

$$\Delta L_{i_3 \to i_4} = L_{i_3}(t) \cdot \frac{F_{i_3 i_4}}{\sum_{o \in N_{i_3}^{neighbor}}^{o} F_{i_3 o}} \tag{26}$$

where i_3 and i_4 are located in the same sub-network, and i_4 is a neighbor node of i_3; $\Delta L_{i_3 \to i_4}$ denotes the load transferred from node i_3 to node i_4; $F_{i_3 i_4}$ denotes the attractiveness between node i_3 and node i_4; $\sum_{o \in N_{i_3}^{neighbor}}^{o} F_{i_3 o}$ denotes the sum of the attractiveness between node i_3 and all its neighbor nodes.

5. Simulation Analysis of Cascading Failures

This paper abstracts real-world scenarios into random attack and deliberate attack scenarios and uses simulation to analyze the vulnerability of the sea-rail cross-border intermodal logistics network when under attack. It also explores the impact of different parameter settings on the vulnerability of the intermodal network, which can provide a theoretical basis for subsequent response strategies.

5.1. Simulation Strategies

A sea–railway cross-border intermodal logistics network is only vulnerable when it is disturbed and experiences node failures. This paper studies the cascading failures in the sea–railway cross-border intermodal logistics network triggered by the failure of a single node, and thereby reveals the vulnerability of the network. This paper abstracts real-world scenarios into random attack and deliberate attack scenarios for simulation purposes. Among them, random attacks mean that the attacker has no clear target, and the attack is characterized by uncertainty. "Emergent events" such as natural disasters and infrastructure failures can be abstracted as random attacks, where natural disasters refer to those that occur in local areas and have a small scope of damage. In the random attack simulation model, it is assumed that all nodes have an identical probability of being disturbed. Each attack occurs randomly on a node in the network, i.e., nodes are randomly selected for removal, with the process iteratively repeated until the network completely collapses. Deliberate attacks refer to intentional actions aimed at key nodes or high-value targets within the network, such as terrorist attacks or the man-made sabotage of critical ports or railway stations. In reality, nodes with high load and high centrality are more likely to be targets of attacks. Therefore, in this paper, the order of node importance calculated by the TOPSIS-entropy weight method in Section 4.3.1 above is used as the order of deliberate attacks. Among them, the top 20 nodes in terms of importance in the sea-rail cross-border intermodal logistics network are shown in Table 3. In the simulation of deliberate attacks, the node with the highest importance in the network is removed in each attack. After removal, the ranking of node importance is updated, and the attack cycle is repeated until the network completely collapses.

This paper uses MATLAB R2016b software to simulate the cascading failure process of the established sea-rail cross-border intermodal logistics network. By drawing trend charts of vulnerability indicators, it compares and analyzes the changes in vulnerability indicators to measure network vulnerability under node failure. Since the simulation experiments involve the selection of random failure thresholds and random attacks, the average result of 20 simulation experiments is taken as a single output value.

Table 3. Ranking of nodes in the intermodal network by importance.

Ranking	Node Name	Node Type	Ranking	Node Name	Node Type
1	Shanghai	Transshipment node	11	Ningbo	Transshipment node
2	Shenzhen	Transshipment node	12	Port Klang	Shipping node
3	Port of Singapore	Shipping node	13	Port of Khor Fakkan	Shipping node
4	Horgos	Railway node	14	Port of Constanza	Shipping node
5	Guangzhou	Transshipment node	15	Yantai	Transshipment node
6	Alataw Pass	Railway node	16	Port Said	Shipping node
7	Qingdao	Transshipment node	17	Mohan	Railway node
8	Tianjin	Transshipment node	18	Hamburg	Transshipment node
9	Manchuria	Railway node	19	Port of Koper	Shipping node
10	Port of Jebel Ali	Shipping node	20	Rotterdam	Shipping node

5.2. Vulnerability Evaluation Indicators

Vulnerability in the field of transportation can be mathematically expressed as the degree of performance degradation of a network after being affected by "unexpected events". This paper employs two indicators, network global efficiency and the largest connected component ratio, to assess the vulnerability of the network.

The first indicator, network global efficiency, is a measure where a higher value generally signifies better network performance. It is calculated using the following formula [66]:

$$E = \frac{2}{n(n-1)} \cdot \sum_{i=1}^{n} \sum_{j=1}^{n} \frac{1}{l_{ij}} \tag{27}$$

where n denotes the total number of nodes in the intermodal network, and l_{ij} denotes the shortest path length between node i and node j.

When a network is subjected to an attack, it can fragment into multiple disconnected components. A component is a subgraph where a path exists between any two nodes. The component containing the most nodes is known as the largest connected component. The largest connected component ratio is used to represent network connectivity. The formula is as follows [67]:

$$LCC = \frac{N'}{N} \tag{28}$$

where N is the number of nodes in the largest connected component of the initial network, and N' is the number of nodes in the largest connected component after the attack.

5.3. Effects of Different Parameters on the Vulnerability of the Intermodal Network

In this paper, the capacity coefficient α represents the optimal processing capacity of a node, and its value mainly depends on the long-term infrastructure planning of the node (such as the number of port berths, the scale of railway hub platforms, etc.). The overload factor θ represents the ultimate bearing capacity of a node, and its value mainly depends on the emergency resources of the node (such as standby equipment, etc.). π represents the load transfer capacity of a transfer node in case of overload or failure, which is an abstract assumption of the transfer mechanism and reflects the load transfer strategy. Since the capacity coefficient α, overload factor θ, and inter-layer transfer probability π respectively reflect the capabilities of nodes at different levels, and their respective determining factors are relatively independent, it is assumed in the modeling process that they can change independently without directly affecting other variables. This paper analyzes the vulnerability of a real-world sea-rail cross-border intermodal logistics network, considering inter-layer transshipment, by employing two distinct attack strategies: random attacks and deliberate attacks based on node centrality. In the parameter settings,

referencing other simulation results [20,68], this paper sets the parameters $\alpha = 0.4$ and $\theta = 1.4$. Additionally, regarding the inter-layer load transfer probability π, it is considered that the proportion of containers transported via sea-rail intermodal transport has reached a maximum of over 40% in some countries [69]. This means that nearly half of the goods can be transported by either maritime or railway transport, and there exists the possibility of mutual substitutability between maritime and railway transport. Based on the above analysis, π is set to 0.5 in this study. This means that the load at a transshipment node has the same probability of being transferred within its layer as it does between layers. Building upon this baseline, the control variable method is then utilized to individually investigate the effects of each parameter on the vulnerability of the intermodal network.

5.3.1. Effect of Capacity Coefficient α on Network Vulnerability

Capacity coefficient α is introduced to adjust the optimal capacity of a node, i.e., the larger the value of α, the greater the total capacity of the node and the higher the load that can be handled by the node. To examine variations in the vulnerability of the sea–railway cross-border intermodal logistics network, this paper controls the value of the capacity coefficient α within the range of [0.1, 0.7] while keeping the values of other parameters constant. Figure 4 shows the simulation results.

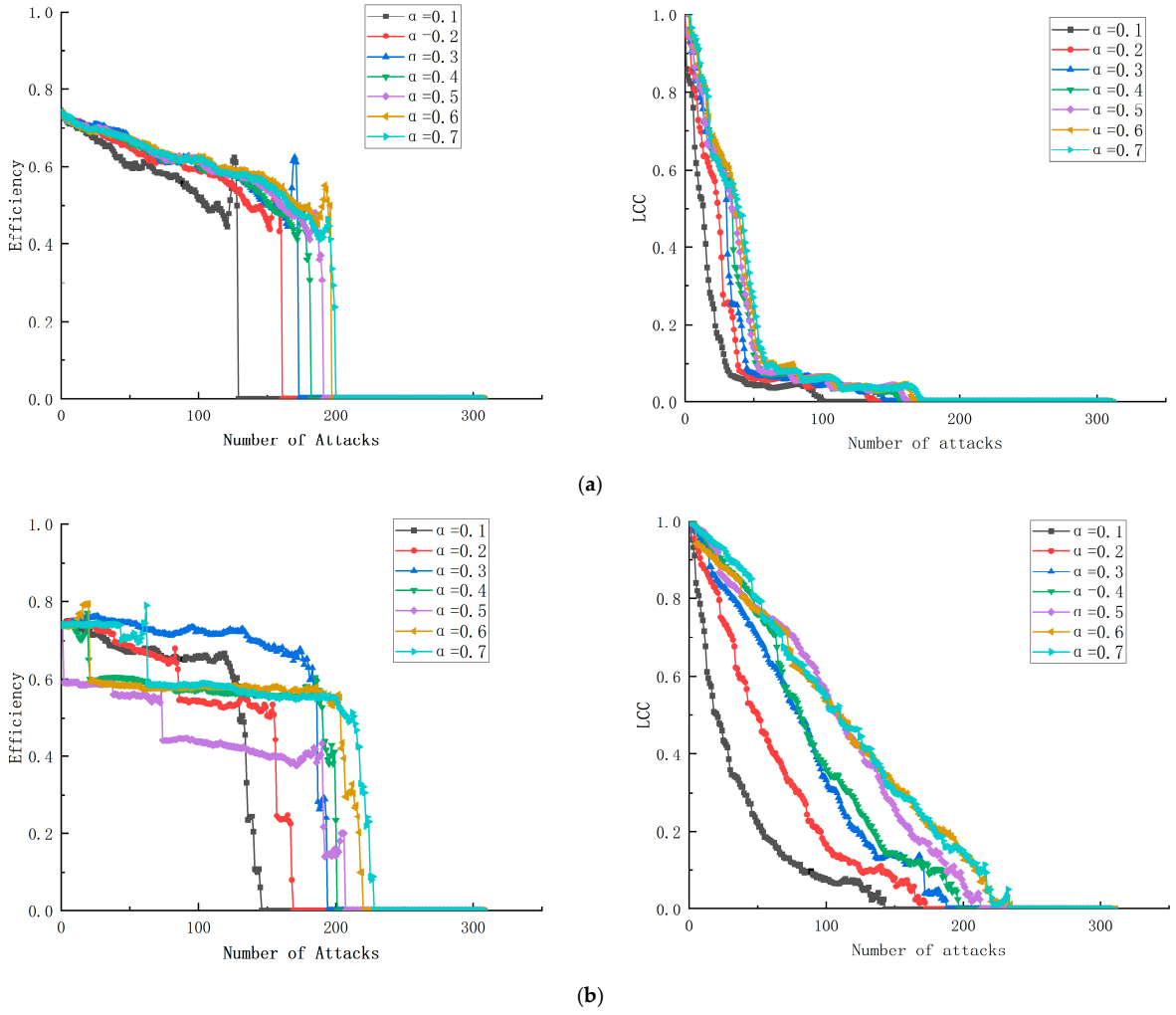

Figure 4. Effect of the parameter α on network vulnerability: (**a**) deliberate attack scenario, (**b**) random attack scenario.

As shown in Figure 4a, under the deliberate attack strategy, the robustness of the sea–railway cross-border intermodal logistics network is progressively enhanced with the increase in the capacity coefficient α. This is specifically manifested by the fact that a larger α value requires a greater number of attacks to reduce the network efficiency and the largest connected component ratio to zero. However, when $\alpha > 0.6$, further increasing its value will not result in any significant variation in the vulnerability level of the intermodal network. It is worth noting that in the network efficiency change curve shown in Figure 4a, a brief rebound in network efficiency occurs. The reason for this phenomenon is that network efficiency is typically defined as the ratio of the sum of the reciprocals of the shortest path lengths between all node pairs to the total number of node pairs. Due to the high redundancy characteristics of the sea-rail cross-border intermodal logistics network, even when the network is attacked and nodes are removed, the remaining nodes can still maintain connectivity through redundant paths, causing the shortest paths between nodes to remain relatively stable. However, as the number of attacked nodes increases, the number of computable node pairs decreases significantly, and the rate at which the number of node pairs decreases exceeds the average rate at which the shortest paths increase, resulting in a temporary rebound in the overall efficiency value [70]. A similar rebound phenomenon can also be observed in Figures 5a, 6a, 7a and 8a. After this brief rebound, the network efficiency rapidly declines as the attack progresses and the network collapses further. As shown in Figure 4b, under the random attack strategy, the decline process of network performance is more gradual compared to that under the deliberate attack. However, the same pattern is revealed under both strategies: appropriately increasing the capacity coefficient α can effectively reduce the network's vulnerability.

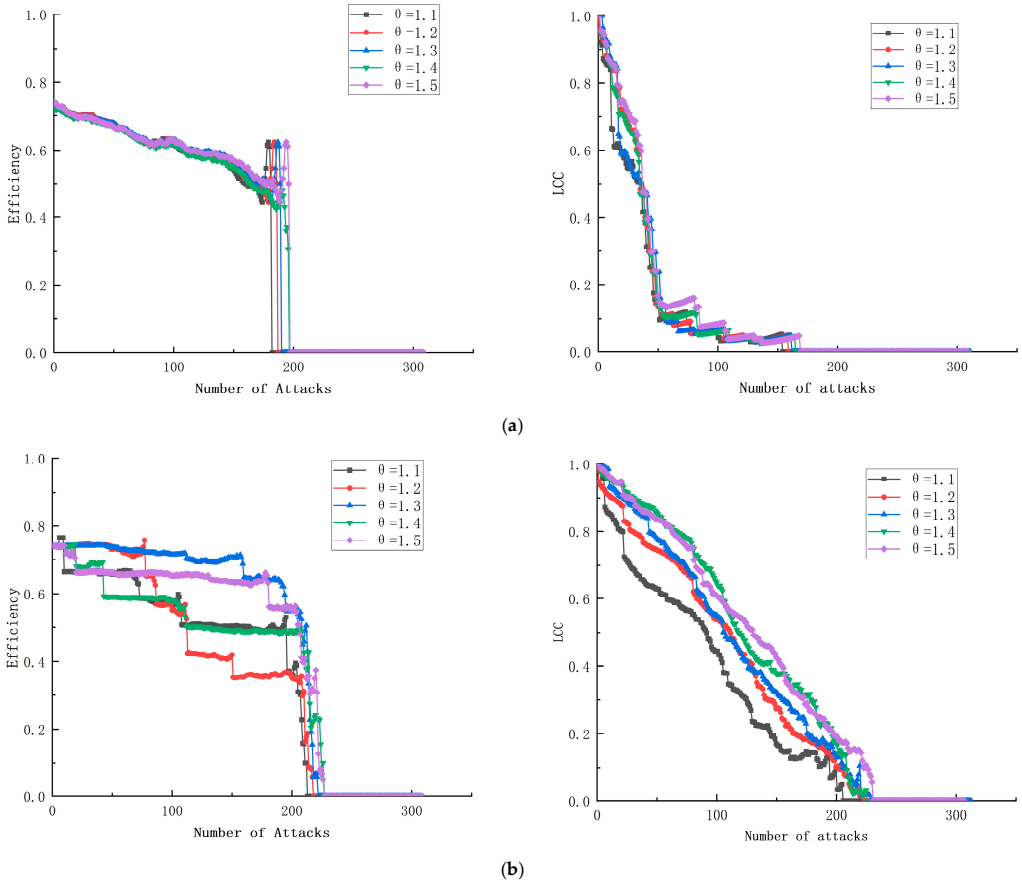

Figure 5. Effect of the parameter θ on network vulnerability: (**a**) deliberate attack scenario, (**b**) random attack scenario.

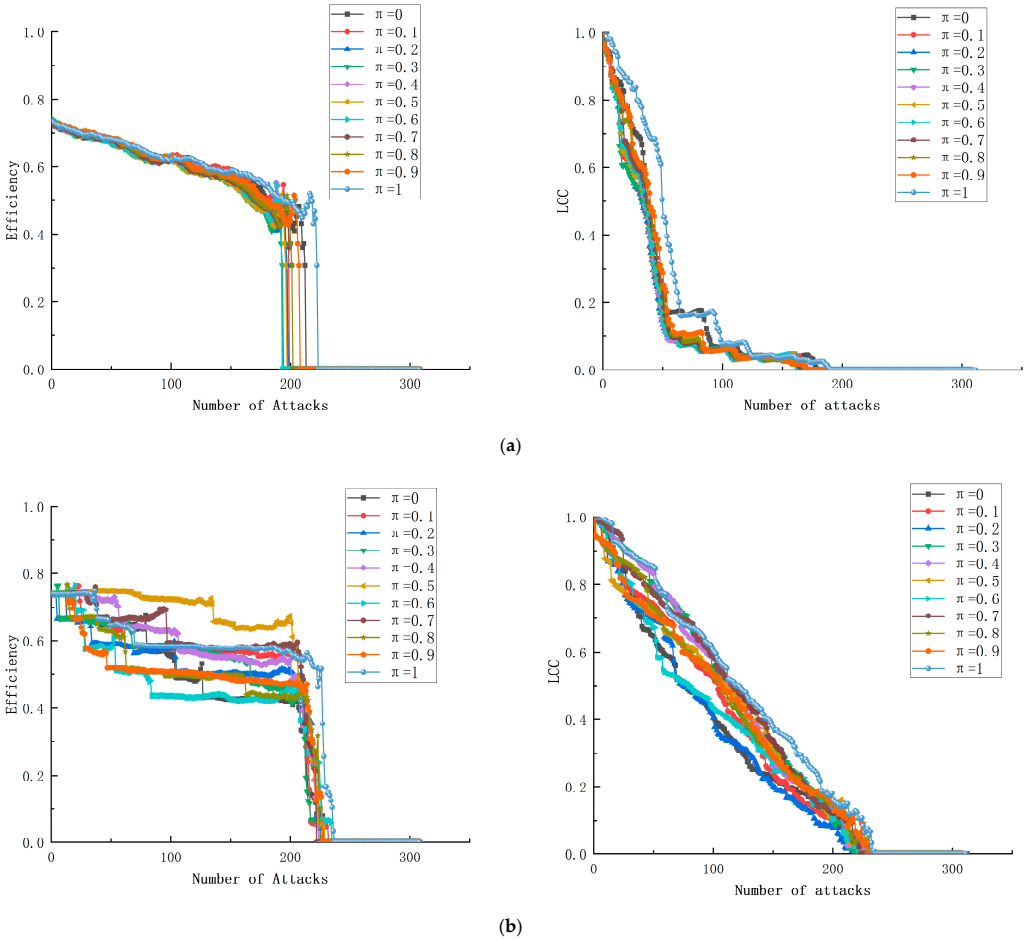

Figure 6. Effect of the parameter π on network vulnerability: (**a**) deliberate attack scenario, (**b**) random attack scenario.

According to a comprehensive consideration of these two attack strategies, the vulnerability level of the intermodal network can be lowered by appropriately increasing the value of the capacity coefficient α. Informed by real-life situations, increasing the capacity coefficient leads to increased construction costs. Thus, the intermodal network can better deal with random and deliberate attacks when the capacity coefficient α = 0.6.

5.3.2. Effect of Overload Factor θ on Network Vulnerability

The overload factor refers to the factor of load-bearing capacity of a node (i.e., a port or railway site). That is, the larger the overload factor, the stronger the load-bearing capacity of the node. To examine the variations in the vulnerability of the sea–railway cross-border intermodal logistics network, this paper controls the value of the overload factor θ within the range of [1.1, 1.5] while keeping the values of all other parameters constant. Figure 5 depicts the simulation results.

As observed in Figure 5, under both the deliberate and random attack strategies, the number of attacks required to reduce both the network efficiency and the largest connected component ratio of the sea-rail cross-border intermodal logistics network to zero indicates that increasing the overload factor θ can effectively enhance the network's robustness against attacks. Upon observing the network efficiency curve under deliberate attacks in Figure 5a, it is found that the efficiency curves for $\theta = 1.4$ and $\theta = 1.5$ almost overlap. This suggests that when $\theta > 1.4$, further increases in θ do not significantly affect the network efficiency.

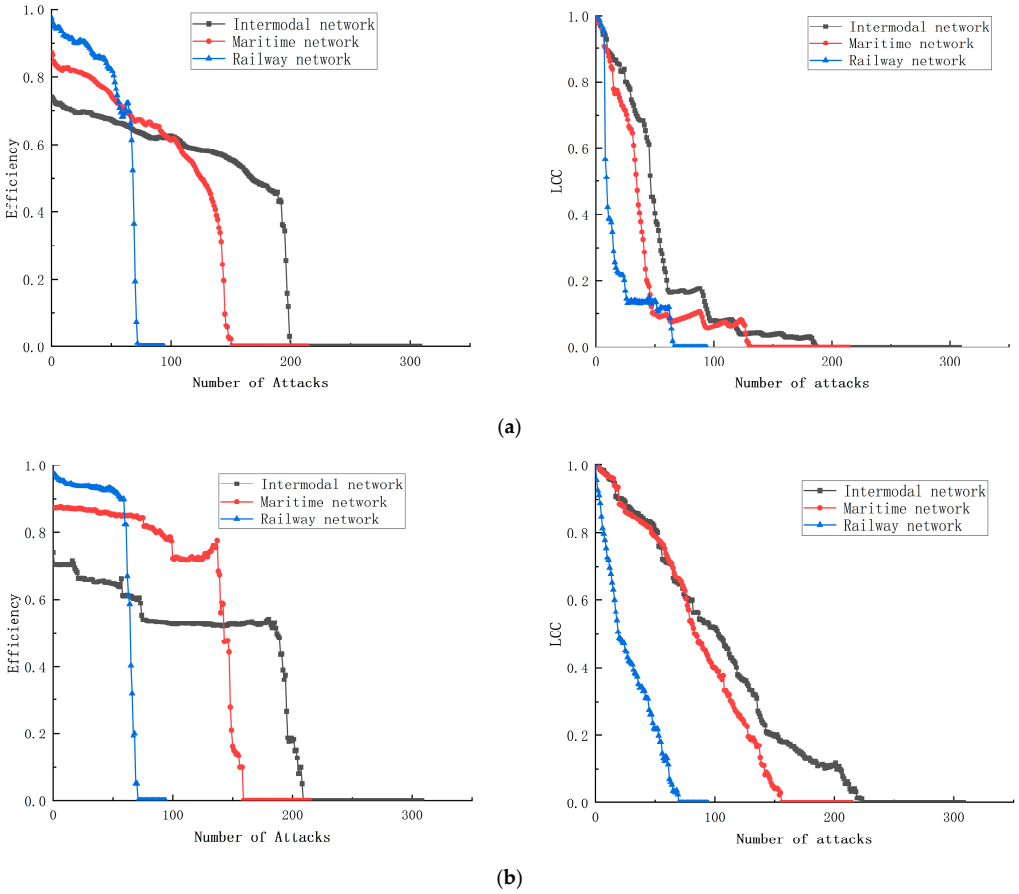

Figure 7. Variations in the efficiency of the intermodal network and its sub-networks: (**a**) deliberate attack scenario, (**b**) random attack scenario.

Overall, the resistance of the intermodal network to deliberate and random attacks can be effectively improved by appropriately increasing the value of the overload factor θ. Moreover, a larger θ can better reflect the anti-attack ability of the network under a high attack intensity. However, when the value of θ is increased to a certain extent, the effect of any further increase will be weakened. Therefore, based on a comprehensive consideration of these two attack strategies, it can be held that, at θ = 1.4, the intermodal network manifests a strong resistance to both types of attacks.

5.3.3. Effect of Inter-Layer Transfer Probability π on Network Vulnerability

The inter-layer transfer probability π refers to the probability of the load of a transshipment node being transferred to another network layer via inter-layer links when the transshipment node fails in a sea–railway intermodal network. To examine the variations in the vulnerability of the sea–railway cross-border intermodal logistics network, this paper controls the value of inter-layer transfer probability π within the range of [0, 1] while keeping the values of other parameters constant. Figure 6 presents the simulation results.

As shown in Figure 6, a comprehensive analysis of both deliberate and random attack strategies indicates that, at $\pi = 1$, the sea–railway cross-border intermodal logistics network exhibits lower vulnerability. The reason for this is that, at $\pi = 1$, the load of the failed transshipment node is entirely transferred to another sub-network. This load redistribution strategy can effectively prevent the overloading and failure of a single network layer. By redistributing the load of the failed transshipment node to another sub-network, the redundancy and unused capacity of the sub-network can be utilized to sustain the efficiency of the entire network. At $\pi = 0$, the load of the failed transshipment node is entirely

redistributed within the current sub-network, preventing the failure of one sub-network from causing the failure of another. This, in turn, enhances the anti-vulnerability capability of the intermodal network as a whole. When π is assigned an intermediate value, each sub-network not only handles its own load but also receives load from other sub-networks, which increases the risk of failure. However, the anti-attack ability of the intermodal network at $\pi = 1$ is stronger than at $\pi = 0$. This is because, at $\pi = 1$, the load of the failed transshipment node is completely transferred to another sub-network, thereby reducing the pressure on a single sub-network, which ultimately strengthens the anti-attack capacity of the entire network. In comparison, at $\pi = 0$, the load of the failed transshipment node is only redistributed within the original sub-network, which can easily lead to node overloading and failure, making the network more vulnerable.

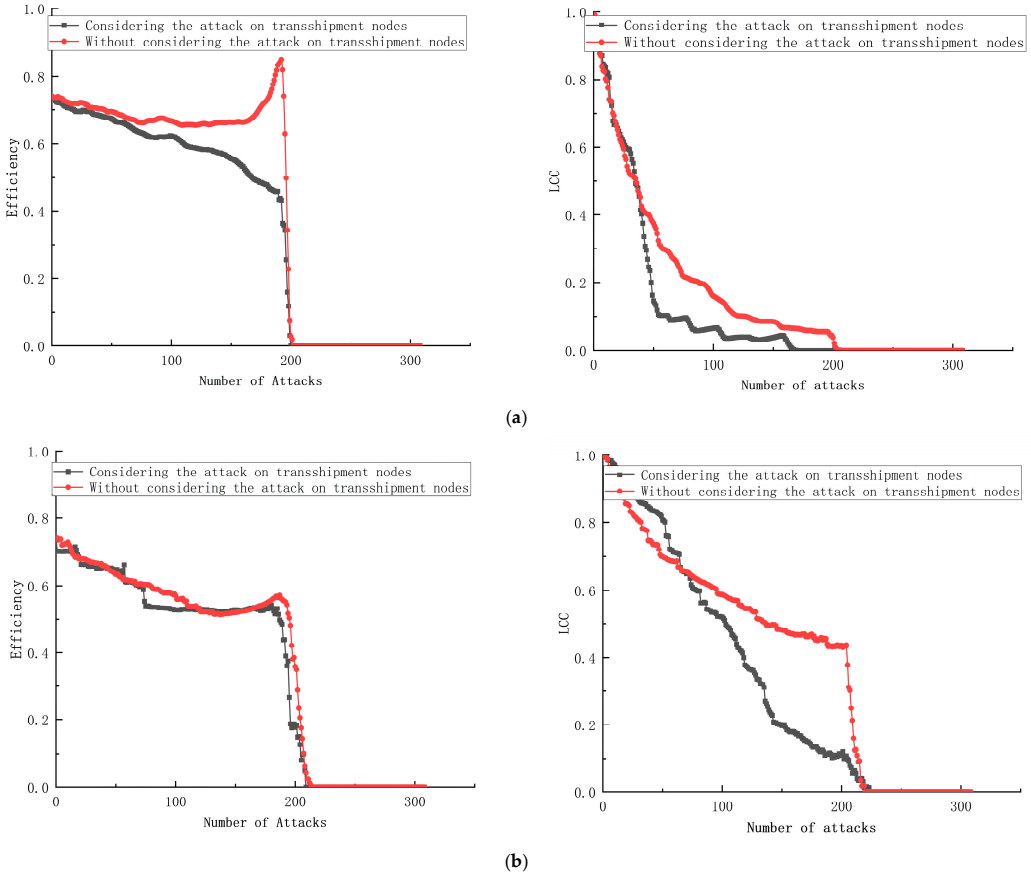

Figure 8. Comparison of variations in the efficiency of the intermodal network, considering and without considering the attack on transshipment nodes: (**a**) deliberate attack scenario, (**b**) random attack scenario.

In brief, the scenario of $\pi = 1$ allows the intermodal network to manifest a stronger resistance to both deliberate and random attacks. Therefore, in a real network, selecting $\pi = 1$ means that, when a node of a certain mode of transport fails, its load can be entirely transferred to another mode of transport, thus enhancing the anti-attack ability of the entire intermodal network. This design strategy ensures that the logistics network can remain stable and efficient in the face of various emergencies and attacks.

5.4. Effects of Different Attack Methods on the Vulnerability of the Intermodal Network and Its Sub-Networks

In the two scenarios of random attacks and node importance-based deliberate attacks, the sea–railway cross-border intermodal logistics network and its maritime and railway

sub-networks are attacked, to comparatively analyze the effects of different attack methods on the vulnerability of the intermodal network and its sub-networks, respectively. The values of parameters remain unchanged. The results are presented in Figure 7.

As shown in Figure 7, under random attack scenarios, the variation trends in network efficiency and the largest connected component ratio for the sea-rail cross-border intermodal logistics network and its sub-networks are more gradual compared to deliberate attacks. However, regardless of whether in deliberate or random attack scenarios, the sea-rail cross-border intermodal logistics network demonstrates lower vulnerability and stronger resistance to attacks compared to its maritime and railway sub-networks. This is because by integrating sea transport and railway transport, the sea–railway cross-border intermodal logistics network has formed a more diversified transport system with more redundancy, which reduces its vulnerability to attacks. By contrast, both maritime and railway networks have exhibited high vulnerability because of their structural singularity. It is worth noting that by virtue of its global connectivity and extensive port coverage, the maritime network can mitigate the impact of attacks to a certain extent; therefore, its vulnerability is lower than that of the railway network.

In short, the intermodal network manifests a stronger anti-attack ability than maritime and railway networks, both in the face of deliberate and random attacks.

5.5. Effect of Transshipment Nodes on Network Vulnerability

In a sea–railway cross-border intermodal logistics network, transshipment nodes serve as key hubs, because their failure may impact more nodes, thereby causing the failure of the entire network. To explore whether the failure of transshipment nodes has a greater impact on the network, the scenario considering the attack on transshipment nodes and the scenario without considering the attack on transshipment nodes under the above two attack strategies were introduced, to comparatively analyze the effects of different scenarios on network vulnerability. The values of parameters are kept unchanged. The results are given in Figure 8.

In addition, to explore the specific impact of the failure of transshipment nodes on the intermodal network, the concept of vulnerability degree [71] was introduced to measure the impact of node failure on network efficiency. This indicator reflects the degree to which network performance is weakened by node failure. Normally, when a node with a higher vulnerability degree fails, the impact on the overall efficiency of the network is more destructive. The formula is as follows:

$$V_i = \frac{E_i - E}{E} \tag{29}$$

where E denotes the original efficiency of the intermodal network, and E_i denotes the network efficiency after the failure of node i.

The top 20 transfer nodes in the sea-rail cross-border intermodal logistics network ranked by their vulnerability, derived from the above analysis, are shown in Table 4.

As shown in Figure 8a, under deliberate attacks, in the sea–railway cross-border intermodal logistics network, compared with the scenario without considering attacks on transshipment nodes, both the network efficiency and the ratio of the largest connected component decline more rapidly when attacks on transshipment nodes are considered. As shown in Figure 8b, in the initial stage of random attacks, the vulnerability indicator declines more slowly under the scenario of considering attacks on transshipment nodes. The possible reason is that, during the early phase of random attacks, most of the removed nodes are of lower importance, exerting only a limited impact on the overall connectivity and efficiency of the network. Consequently, the network structure remains relatively stable. However, as the number of attacks increases, some critical transshipment nodes are

eventually targeted, the core hub functions of the network are impaired, and its performance declines more rapidly in the later stages.

Table 4. Measurement results of comparison of variations in the efficiency of the intermodal network, considering and without considering the attack on transshipment nodes.

	Name of Transshipment Node	Ranking by Vulnerability Degree	Vulnerability Degree		Name of Transshipment Node	Ranking by Vulnerability Degree	Vulnerability Degree
1	Port of Shenzhen	3	0.0057	11	Shenzhen (railway node)	71	0.0011
2	Port of Dalian	11	0.0036	12	Shanghai (railway node)	73	0.0011
3	Port of Fuzhou	17	0.0031	13	Port of Haiphone	87	0.0008
4	Port of Tianjin	20	0.0027	14	Tianjin (railway node)	96	0.0007
5	Port of Guangzhou	35	0.0022	15	Port of Qinzhou	97	0.0007
6	Fuzhou (railway node)	48	0.0016	16	Ho Chi Minh (railway node)	99	0.0007
7	Qingdao (railway node)	54	0.0015	17	Bangkok (railway node)	103	0.0006
8	Port of Xiamen	59	0.0013	18	Port of Lianyungang	104	0.0006
9	Port of Bangkok	61	0.0013	19	Lianyungang (railway node)	106	0.0006
10	Port of Shanghai	70	0.0011	20	Port of Hamburg	115	0.0004

In summary, in the sea–railway cross-border intermodal logistics network, transshipment nodes serve as critical hubs and are essential for maintaining the network's global efficiency and connectivity. Their failure significantly increases the vulnerability of the network. Therefore, enhancing the protection of transshipment nodes is a crucial approach to reducing the vulnerability of the sea–railway cross-border intermodal logistics network.

The ranking of transshipment nodes by vulnerability degree reflects the impact of their failures on the overall efficiency of the network. As shown by the data in Table 4, the Port of Shenzhen and the Port of Dalian are the most critical transshipment nodes that play very prominent pivotal roles and have relatively high vulnerability degrees in the network. This means that, once they fail, not only will local nodes in the maritime or railway network be affected, but also the transfer and flow of cargoes between different network layers will be impacted.

Given that transshipment nodes play a key role in sea–railway cross-border intermodal logistics networks, effective measures must be taken to reduce their vulnerability. Taking the Port of Shenzhen, a key transshipment node, as an example, considering the more direct effects of the capacity coefficient α, overload factor θ, and inter-layer transfer probability π on the daily operation of the transshipment node, in this paper, the effects of these three parameters on the vulnerability of the transshipment node are analyzed through simulation. On this basis, strategies and measures to reduce the vulnerability of the transshipment node are proposed. The simulation results are shown in Figures 9–11.

Combining Figures 9 and 10 shows that with increasing capacity coefficient α and overload factor θ, the vulnerability of the transshipment node generally presents a downward trend. This indicates that the transshipment node can handle larger cargo flows and has a significantly reduced vulnerability after the increase in its capacity and the enhancement of its overload-bearing capacity. This result further suggests that increasing the capacity of a transshipment node offers an effective way to reduce its vulnerability. Observing Figure 11 shows that, under a low inter-layer transfer probability, the transshipment node is prone to load concentration, resulting in a higher vulnerability degree. With increasing inter-layer transfer probability, the load of the transshipment node is effectively dispersed, and its vulnerability is gradually reduced. This result suggests that increasing the inter-

layer transfer probability can effectively alleviate the load pressure of transshipment nodes and enhance their anti-risk ability.

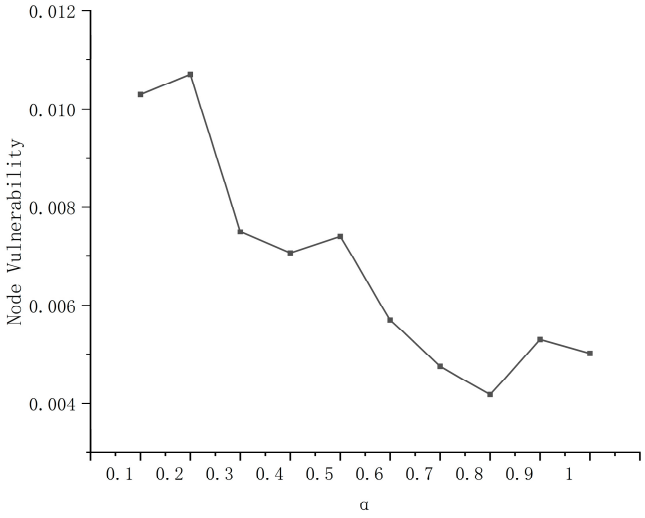

Figure 9. Impact of the capacity coefficient α on the vulnerability degree of transshipment nodes.

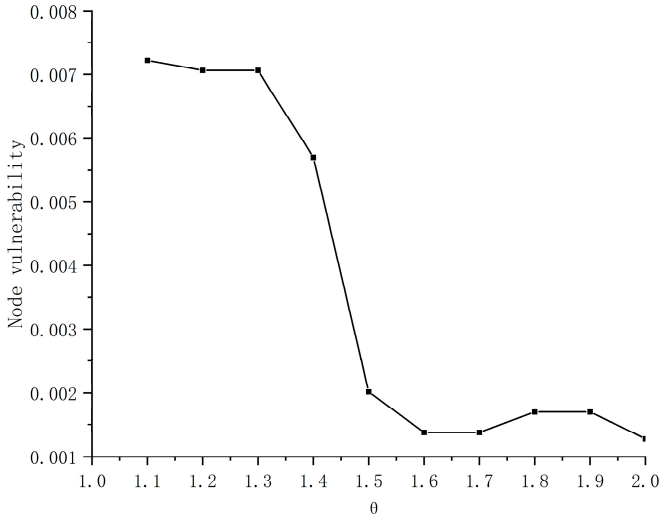

Figure 10. Impact of the overload factor θ on the vulnerability degree of transshipment nodes.

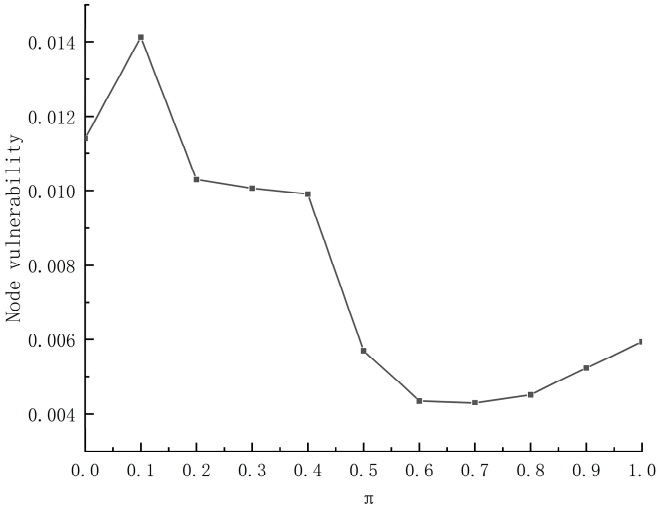

Figure 11. Impact of the inter-layer transfer probability π on the vulnerability degree of transshipment nodes.

6. Conclusions

Relying on shipping and railway data, in this paper, a sea–railway cross-border intermodal logistics network composed of maritime and railway networks via transshipment nodes is constructed first. Then, on the basis of the network being a complex network characterized by scale-free property, high cluster coefficient, and short average path length, a cascading failure model considering inter-layer transshipment is proposed based on complex network theories, the cascading failure model, and the modified logistics attractiveness model. The spread characteristics of the network are considered under the impacts of intra-layer and inter-layer logistics transport between network nodes. Finally, the vulnerability of the sea–railway cross-border intermodal logistics network is analyzed under both deliberate attack and random attack strategies.

The main conclusions are summarized as follows: First, through simulation, it is found that when the capacity coefficient $\alpha = 0.6$, overload factor $\theta = 1.4$, and inter-layer transshipment probability $\pi = 1$, the sea-rail cross-border intermodal logistics network can better cope with random attacks and deliberate attacks, and the network vulnerability is lower under this condition. Specifically, although a larger capacity coefficient and overload factor can enhance the resistance of the sea-rail cross-border intermodal logistics network against attacks, in practical applications, increasing the capacity coefficient requires expanding infrastructure (such as ports and railway platforms), and increasing the overload factor necessitates investing more in standby facilities, which is accompanied by higher construction and maintenance costs. A reasonable approach is to moderately increase the capacity coefficient and overload factor on the premise that the network vulnerability is effectively controlled, so as to achieve a balance between performance optimization and cost control. Similarly, an inter-layer transfer probability of $\pi = 1$ means complete load transfer, which requires sufficient transfer facilities. Its feasibility in practical applications may be limited, so the network can be made to move closer to this ideal state. These conclusions provide a direction for improving the invulnerability of the network. Second, the sea–railway cross-border intermodal logistics network and its maritime and railway network show high vulnerability under the deliberate attack strategy, but low vulnerability under the random attack strategy. Compared with its two sub-networks, the sea–railway cross-border intermodal logistics network manifests a lower vulnerability and a stronger anti-attack ability. Among these three, the railway network has the highest vulnerability. Finally, attacking transshipment nodes under the deliberate attack strategy will more likely lead to the cascading failure of the sea–railway cross-border intermodal logistics network. The vulnerability of transshipment nodes can be reduced by increasing the capacity coefficient, the overload factor, and the inter-layer transfer probability.

These findings provide some insights for logistics operators, port management agencies, and policymakers. First, in the construction of ports and railway platforms, attention should be paid to improving the redundancy of infrastructure to cope with unexpected events. In particular, more investment should be made in protecting and strengthening some key nodes in the network, such as important transit nodes like Shenzhen Port and Dalian Port. Second, in the planning of logistics networks, full consideration should be given to integrating multiple transportation modes to enhance the invulnerability of the overall network. Meanwhile, it is necessary to improve the construction of corridors between railways and ports to ensure the smooth and efficient transfer of goods between different transportation modes. To further enhance the coordination between various transportation modes and the efficiency of information flow, intelligent technologies such as automated container transfer systems and smart logistics platforms can be introduced, which will significantly strengthen the flexibility and operational efficiency of the network.

Third, when allocating emergency resources, priority should be given to transfer nodes with high vulnerability in the network.

However, it is also important to point out the limitations of this paper. In real-world sea-rail cross-border intermodal logistics networks, inter-layer transfers involve processes such as cargo loading and unloading, transshipment transportation, and temporary storage, which are usually accompanied by the generation of time and costs. In this paper, the modeling of "inter-layer transshipment" is simplified, with the aforementioned factors neglected. Furthermore, to reduce the complexity of the model, cargo attributes are disregarded, and goods are abstracted as standardized load units. These simplifications may impose certain limitations on the simulation. First, the model ignores the time required for inter-layer transshipment, and the vulnerability analysis results may be inaccurate due to the failure to consider dynamic time factors. Future research can consider incorporating transshipment time factors to accurately analyze the impact of inter-layer transshipment time on network vulnerability. Second, the model in this paper ignores the costs incurred by transshipment nodes during inter-layer transshipment, making it unable to accurately describe the actual operational pressure on these nodes. Future research should consider setting resource constraints for each transshipment node to better align with real-world scenarios. Third, the model simplifies goods into standardized load units and ignores cargo characteristics, which may lead to unreasonable route selection. Future research should focus on cargo attributes and select appropriate transportation modes based on the priority and transportation needs of different cargo types. Finally, for a more comprehensive and realistic assessment, future work should extend the current model by incorporating edge failures (such as shipping route disruptions), thereby addressing the limitation of focusing solely on node failures.

Author Contributions: Conceptualization, H.W.; methodology, H.W. and H.Q.; validation, H.Q.; investigation, H.W. and H.Q.; data curation, H.W. and H.Q.; writing—original draft preparation, H.W. and H.Q.; writing—review and editing, H.W. and H.Q.; visualization, H.Q.; supervision, H.W.; funding acquisition, H.W. All authors have read and agreed to the published version of the manuscript.

Funding: This study was funded by the National Social Science Foundation of China (Grant No. 24CGL039). The authors gratefully acknowledge the financial support.

Data Availability Statement: The data are available from the corresponding author on reasonable request.

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

References

1. Boccaletti, S.; Bianconi, G.; Criado, R.; del Genio, C.I.; Gomez-Gardenes, J.; Romance, M.; Sendina-Nadal, I.; Wang, Z.; Zanin, M. The structure and dynamics of multilayer networks. *Phys. Rep.* **2014**, *544*, 1–122. [CrossRef]
2. The Red Sea Crisis Disrupts Global Supply Chains, But the China-Europe Railway Takes Over. Jingyang Brewery. 2024. Available online: https://baijiahao.baidu.com/s?id=1789672342734784027&wfr=spider&for=pc (accessed on 19 March 2025).
3. Case Study 12: Port of New York, United States. Available online: https://resilientmaritimelogistics.unctad.org/guidebook/case-study-12-port-new-york-united-states (accessed on 18 June 2025).
4. Wan, Z.; Su, Y.; Li, Z.; Zhang, X.; Zhang, Q.; Chen, J. Analysis of the impact of Suez Canal blockage on the global shipping network. *OCEAN Coast. Manag.* **2023**, *245*, 106868. [CrossRef]
5. Xia, M.; Chen, J.; Zhang, P.; Peng, P.; Claramunt, C. Spatial Structure and Vulnerability of Container Shipping Networks: A Case Study in the Beibu Gulf Sea Area. *J. Mar. Sci. Eng.* **2024**, *12*, 1307. [CrossRef]
6. Zhang, Z.J.; Zhang, Y.Z.; Wang, X.R. Robustness analysis of railway express freight network. *Chin. Saf. Sci. J.* **2020**, *30*, 150–156. [CrossRef]
7. Xu, F.; Miao, J.J. The Robustness of High-Speed Railway and Civil Aviation Compound Network Based on the Complex Network Theory. *Complex Syst. Complex. Sci.* **2015**, *12*, 40–45. [CrossRef]

8. Du, Q.; Kishi, K.; Nakatsuji, T. Vulnerability Evaluation of Logistice Transportaion Networks Under Seismic Disasters. *Transp. Res. Rec.* **2015**, *2532*, 45–55. [CrossRef]
9. The Vulnerability of the European Air Traffic Network to Spatial Hazards. Natural Hazards. Available online: https://link.springer.com/article/10.1007/s11069-011-9885-6 (accessed on 29 June 2025).
10. Erol, S. The early impact of the Russia-Ukraine war on seaborne trade and transportation in the Black Sea. *Int. J. Shipp. Transp. Logist.* **2024**, *18*, 305–323. [CrossRef]
11. Li, D.Y.H.; Jiao, J.B.; Wang, S.Y.; Zhou, G.H. Impact of Global Key Shipping Lane Blockages on Supply Chains: A Case Study of the "Ever Given" Grounding in the Suez Canal. *Manag. Rev.* **2025**, *37*, 237–248. [CrossRef]
12. Jiang, M.Z.; Lu, J.; Qu, Z.; Yang, Z.L. Port vulnerability assessment from a supply Chain perspective. *Ocean Coast. Manag.* **2021**, *213*, 105851. [CrossRef]
13. Guo, J.K.; Feng, T.Q.; Wang, S.B.; Qin, Y.F.; Yu, X.H. Shipping network vulnerability assessment integrated with geographical locations. *Transp. Res. PART-Transp. Environ.* **2024**, *130*, 104166. [CrossRef]
14. Wen, T.; Gao, Q.; Chen, Y.; Cheong, K.H. Exploring the vulnerability of transportation networks by entropy: A case study of Asia–Europe maritime transportation network. *Reliab. Eng. Syst. Saf.* **2022**, *226*, 108578. [CrossRef]
15. Zhou, Y.; Kundu, T.; Qin, W.; Goh, M.; Sheu, J.-B. Vulnerability of the worldwide air transportation network to global catastrophes such as COVID-19. *Transp. Res. PART E-Logist. Transp. Rev.* **2021**, *154*, 102469. [CrossRef] [PubMed]
16. Wu, D.; Wang, Y.P.; Sheng, S.J.; Wang, N. Vulnerability changes of the Maritime Silk Road container shipping network under intentional attacks. *Acta Geogr. Sin.* **2022**, *77*, 2067–2082. [CrossRef]
17. Baggag, A.; Abbar, S.; Zanouda, T.; Srivastava, J. Resilience analytics: Coverage and robustness in multi-modal transportation networks. *EPJ DATA Sci.* **2018**, *7*, 14. [CrossRef]
18. Zheng, Z.H.; Huang, Z.R.; Zhang, F.; Wang, P. Understanding coupling dynamics of public transportation networks. *EPJ DATA Sci.* **2018**, *7*, 23. [CrossRef]
19. Zhang, X.; Li, S.F.; Sun, D.Y. Vulnerability Analysis of China-Europe Container Sea-rail Intermodal Transport Network. *J. Transp. Inf. Saf.* **2023**, *41*, 48–58. [CrossRef]
20. Zhang, Y.Z.; Kang, H.H.; Zhang, Y.L. Vulnerability analysis of cascading failure of Sino-Europe sea-rail transport network from the perspective of multi-layer network. *Comput. Eng. Appl.* **2025**, *61*, 298–308. [CrossRef]
21. Xiong, Q.; Xu, B.; Li, J. Risk–Failure Interactive Propagation and Recovery of Sea–Rail Intermodal Transportation Network Considering Recovery Propagation. *J. Mar. Sci. Eng.* **2025**, *13*, 781. [CrossRef]
22. Lu, Z.; Qiu, W. Resilience Analysis of Seaport–Dry-Port Network in Container Transport: Multi-Stage Load Redistribution Dynamics Following Cascade Failure. *Systems* **2025**, *13*, 299. [CrossRef]
23. Feng, F.L.; Dong, K.Y.; Zhang, Z.; Fang, Y. Analysis of Vulnerability for New Western Land-sea Corridor Network Based on Cascading Failures. *J. Transp. Syst. Eng. Inf. Technol.* **2024**, *24*, 15–29. [CrossRef]
24. Wang, Y.G.; Wang, L.J.; Liu, Z.G.; Ren, L. Vulnerability metrics of multimodal composite transportation network. *J. Traffic Transp. Eng.* **2023**, *23*, 195–207. [CrossRef]
25. Ferrari, C.; Santagata, M. Vulnerability and robustness of interdependent transport networks in north-western Italy. *Eur. Transp. Res. Rev.* **2023**, *15*, 6. [CrossRef]
26. Ippolito, N.; Cats, O. Multi-modal and multi-layer robustness analysis of the European rail and air networks. *Sci. Rep.* **2024**, *14*, 26950. [CrossRef]
27. Boura, G.; Ferguson, N.S. Incorporating geographic interdependencies into the resilience assessment of multimodal public transport networks. *J. Transp. Geogr.* **2024**, *118*, 103934. [CrossRef]
28. Yang, Y.; Li, G.Y. Identification of Critical Nodes and Damage Resistance Analysis of Road Network in Mountainous Areas under Natural Disasters. *J. Catastrophol.* **2024**, 87–93. [CrossRef]
29. Sun, R.R.; Zhu, G.Y.; Liu, B.; Li, X.L.; Yang, Y.Y.; Zhang, J.X. Vulnerability Analysis of Urban Rail Transit Network considering Cascading Failure Evolution. *J. Adv. Transp.* **2022**, *2022*, 2069112. [CrossRef]
30. Gao, L.; Liu, X.Q.; Liu, Y.; Wang, P.; Deng, M.; Zhu, Q.; Li, H. Measuring road network topology vulnerability by Ricci curvature. *Phys. Stat. Mech. Appl.* **2019**, *527*, 121071. [CrossRef]
31. Sohouenou, P.Y.R.; Christidis, P.; Christodoulou, A.; Neves, L.A.C.; Presti, D.L. Using a random road graph model to understand road networks robustness to link failures. *Int. J. Crit. Infrastruct. Prot.* **2020**, *29*, 100353. [CrossRef]
32. Shen, Z.; Xu, X.; Li, J.; Wang, S. Vulnerability of the Maritime Network to Tropical Cyclones in the Northwest Pacific and the Northern Indian Ocean. *Sustainability* **2019**, *11*, 6176. [CrossRef]
33. 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.* **2019**, *229*, 106325. [CrossRef]
34. Chen, H.; Zhang, L.; Liu, Q.; Wang, H.; Dai, X. Simulation-based vulnerability assessment in transit systems with cascade failures. *J. Clean. Prod.* **2021**, *295*, 126441. [CrossRef]

35. Wu, Y.; Chen, Z.; Zhao, X.; Liu, Y.; Zhang, P.; Liu, Y. Robust analysis of cascading failures in complex networks. *Phys.-Stat. Mech. Appl.* **2021**, *583*, 126320. [CrossRef]
36. Guo, J.N.; Xu, J.X.; He, Z.G.; Liao, W. Research on risk propagation method of multimodal transport network under uncertainty. *Phys. Stat. Mech. Appl.* **2021**, *563*, 125494. [CrossRef]
37. Duan, X.H.; Xu, X.; Tang, J. Study on vulnerability evolution of urban integrated passenger transport hub based on weighted CML. *J. Saf. Sci. Technol.* **2023**, *19*, 186–191. [CrossRef]
38. Xiong, Z.H.; Yao, Z.S. Influence Scope of Cascading Failure on Rail Transit System. *J. Transp. Syst. Eng. Inf. Technol.* **2020**, *20*, 12–18. [CrossRef]
39. Hassan, R.; Yosri, A.; Ezzeldin, M.; El-Dakhakhni, W. Robustness Quantification of Transit Infrastructure under Systemic Risks: A Hybrid Network-Analytics Approach for Resilience Planning. *J. Transp. Eng. PART Syst.* **2022**, *148*, 04022089. [CrossRef]
40. Xu, J.Q.; Huang, H.N.; Cheng, Y.Q.; Chen, K.M. Vulnerability assessment of freeway network considering the probabilities and consequences from a perspective based on network cascade failure. *PLoS ONE* **2022**, *17*, e0265260. [CrossRef]
41. Guo, Z.J.; Wang, Y.; Zhong, J.L.; Fu, C.Q.; Sun, Y.; Li, J.; Chen, Z.; Wen, G. Effect of load-capacity heterogeneity on cascading overloads in networks. *CHAOS* **2021**, *31*, 123104. [CrossRef]
42. Tian, W.; Zhou, X.F.; Fang, Q.; Song, J.J. Vulnerability analysis of en-route network based on cascading failure. *J. Southwest Jiaotong Univ.* **2023**, 317–325. [CrossRef]
43. Motter, A.E.; Lai, Y.-C. Cascade-based attacks on complex networks. *Phys. Rev. E* **2002**, *66*, 065102. [CrossRef] [PubMed]
44. Watts, D.J. A simple model of global cascades on random networks. *Proc. Natl. Acad. Sci. USA* **2002**, *99*, 5766–5771. [CrossRef]
45. Weng, W.G.; Ni, S.J.; Yuan, H.Y.; Fan, W.C. Modeling the dynamics of disaster spreading from key nodes in complex networks. *Int. J. Mod. Phys. C* **2007**, *18*, 889–901. [CrossRef]
46. Li, C.D.; Deng, Y.; Yuan, Z.; Feng, W.Y. Dynamic Information-Based Load Reallocation Strategy for Cascading Failure Networks. *J. South China Univ. Technol. Nat. Sci. Ed.* **2016**, *44*, 22–28. [CrossRef]
47. Hong, C.; Zhang, J.; Du, W.B.; Sallan, J.M.; Lordan, O. Cascading failures with local load redistribution in interdependent Watts-Strogatz networks. *Int. J. Mod. Phys. C* **2016**, *27*, 1650131. [CrossRef]
48. Hao, Y.C.; Jia, L.M.; Wang, Y.H.; He, Z.C. Modelling cascading failures in networks with the harmonic closeness. *PLoS ONE* **2016**, *16*, e0243801. [CrossRef]
49. Wang, L.F.; Li, H.; Zhao, G.T. Improved Load Re-allocation Strategy Based on Maximum Residual Capacity of Node. *J. Northeast. Univ. Nat. Sci.* **2020**, *41*, 1223–1230. [CrossRef]
50. Wang, C.F.; Wang, D.L. Safety influencing factors of transmission line crossover construction: Based on improved DEMATEL. *J. Saf. Environ.* **2022**, *22*, 43–50. [CrossRef]
51. Liang, Z.Q.; Fu, D.L.; Deng, Y. A load redistribution strategy based on dynamic information in cascading process. *Comput. Eng. Sci.* **2017**, *39*, 1638–1644. [CrossRef]
52. Lu, B.; Sun, Y.; Wang, H.; Wang, J.-J.; Liu, S.S.; Cheng, T.C.E. Dynamic resilience analysis of the liner shipping net-work: From structure to cooperative mechanism. *Transp. Res. Part E Logist. Transp. Rev.* **2024**, *191*, 103755. [CrossRef]
53. Cumelles, J.; Lordan, O.; Sallan, J.M. Cascading failures in airport networks. *J. Air Transp. Manag.* **2021**, *92*, 102026. [CrossRef]
54. Ge, J.W.; Wang, X.F.; Wan, Z.; Huang, T.R. Community Structure of World Container Shipping Network. *J. Transp. Syst. Eng. Inf. Technol.* **2019**, *19*, 231–236. [CrossRef]
55. Wang, X.F.; Li, X.; Chen, G.R. *Network Science: An Introduction*; Higher Education Press: Beijing, China, 2012; Volume 4, pp. 95–142.
56. von Ferber, C.; Holovatch, T.; Holovatch, Y.; Palchykov, V. Public transport networks: Empirical analysis and modeling. *Eur. Phys. J. B* **2009**, *68*, 261–275. [CrossRef]
57. Lai, Y.C.; Motter, A.E.; Nishikawa, T. Attacks and Cascades in Complex Networks. In *Complex Networks*; Ben-Naim, E., Frauenfelder, H., Toroczkai, Z., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; pp. 299–310. [CrossRef]
58. Resource Allocation Pattern in Infrastructure Networks—IOPscience. Available online: https://iopscience.iop.org/article/10.1088/1751-8113/41/22/224019 (accessed on 8 July 2025).
59. Xu, B.W.; Tang, C.X.; Li, J.J. Robustness Analysis of Seaport-dry Port Container Transport Networks Under Cascading Failure. *J. Transp. Syst. Eng. Inf. Technol.* **2023**, *23*, 265–279. [CrossRef]
60. Li, Q.X.; Jin, F.H.; Sun, P.S. Construction and Application of Regional Logistics Gravity Model and Regional Logistics Status Model. *Econ. Geogr.* **2010**, *30*, 1619–1624+1630. [CrossRef]
61. Ma, L.L.; Ma, C.; Zhang, H.F.; Wang, B.H. Identifying influential spreaders in complex networks based on gravity formula. *Phys. Stat. Mech. Appl.* **2016**, *451*, 205–212. [CrossRef]
62. Wang, D.F.; Dong, Q.L.; Chen, Y.; Sun, M.P. Analysis of the logistics network structure of urban along the China Railway Express. *Resour. Environ. Yangtze Basin.* **2018**, *27*, 32–40. [CrossRef]
63. Xue, F.; He, C.-L.; Sun, Z.-S.; Yu, X. Key Node Identification Method of Chengdu Metro Network Based on Comprehensive Assessment. In *Advances in Smart Vehicular Technology, Transportation, Communication and Applications*; Ni, S., Wu, T.Y., Chang, T.H., Pan, J.S., Jain, L.C., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 48–58. [CrossRef]

64. Chen, W.; Zou, S.; Qiu, C.; Dai, J.; Zhang, M. Invulnerability analysis of nuclear accidents emergency response organization network based on complex network. *Nucl. Eng. Technol.* **2024**, *56*, 2923–2936. [CrossRef]
65. Yu, H.; Liu, Z.; Li, Y.J. Key nodes in complex networks identified by multi-attribute decision-making method. *Acta Phys. Sin.* **2013**, *62*, 54–62. [CrossRef]
66. Lyu, M.; Shuai, B.; Zhang, Q.Y.; Li, L.Q. Ripple effect in China–Europe Railway transport network: Ripple failure risk propagation and influence. *Phys. Stat. Mech. Appl.* **2023**, *620*, 128739. [CrossRef]
67. Bombelli, A.; Santos, B.F.; Tavasszy, L. Analysis of the air cargo transport network using a complex network theory perspective. *Transp. Res. Part E-Logist. Transp. Rev.* **2020**, *138*, 101959. [CrossRef]
68. Shan, X.H. Research on the Invulnerability of Urban Composite Transportation Network Based on Coupled Network. Master's Thesis, Dalian Jiaotong University, Dalian, China, 2024. [CrossRef]
69. Ministry of Transport Promotes Multimodal Transport to Enhance the Capacity of the "Belt and Road" Initiative—Belt and Road Portal of China. Available online: https://www.yidaiyilu.gov.cn/p/36187.html (accessed on 26 September 2025).
70. Wang, Z.H.; Hu, W.Q.; Wang, Y.W. Resilience Assessment of Yangtze River Delta and Guangdong-Hong Kong-Macao Shipping Networks Based on Complex Network. *J. Transp. Syst. Eng. Inf. Technol.* **2023**, *23*, 184–193. [CrossRef]
71. Wu, S.; Han, X.L.; Liu, C.J.; Hu, Z.H. Vulnerability analysis of global container shipping network based on complex network. *Comput. Eng. Appl.* **2018**, *54*, 249–254. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.