Exploring the vulnerability of transportation networks by entropy: A case study of Asia–Europe maritime transportation network

DOI:
10.1016/j.ress.2022.108578

Document Version
Accepted author manuscript

Exploring the Vulnerability of Transportation Networks by Entropy: A Case Study of Asia-Europe Maritime Transportation Network

Tao Wen[a], Qiuya Gao[a], Yu-wang Chen[b], Kang Hao Cheong[a,c,*]

[a]*Science, Mathematics and Technology Cluster, Singapore University of Technology and Design (SUTD), S487372, Singapore*
[b]*Alliance Manchester Business School, The University of Manchester, Manchester M15 6PB, UK*
[c]*SUTD-Massachusetts Institute of Technology International Design Centre, S487372, Singapore*

Abstract

With the rise of global trade, maritime transportation networks have become an indispensable element of logistics networks. Approximately 80% of the global trade volume is transported by sea with the maritime logistics network fuelling global economic integration. Due to the uncertainty of the transportation process and the impact of accidents, the reliability analysis of the logistics network is a topic of immense interest. In this paper, we propose an original and novel model to quantitatively analyze the vulnerability of the maritime logistics network by considering the importance of each port in the network. Three centrality measures that consider different topology information of the network are used in this paper to identify the importance of ports. Different information about the network is considered through the joint entropy and the multiscale factor q to evaluate the vulnerability of the logistics network. The Asia-Europe maritime transportation network serves as a real-world example to demonstrate the effectiveness and applicability of our proposed model. The experimental results suggest that the performance of the maritime network is closely related to the heterogeneity of the connectivity pattern and the process of decentralization can reduce the vulnerability of the maritime network.

Keywords: Transportation Networks, Network Theory, Joint Entropy, Vulnerability, Centrality

1. Introduction

The usage of transportation network has become an indispensable part of daily life [1, 2]. Short-distance cars, long-distance trains, and transoceanic planes are common across travel patterns. Due to globalization and the development of maritime transportation, people can now easily enjoy commodities from all over the world without long-distance travel [3]. Therefore, the performance analysis and planning of the transportation system is a topic of immense interest among researchers. When the city (port, or station) is regarded as a node and the connection (transportation) between them is regarded as a connecting edge, such a complex system can be modeled by complex network to better understand its characteristics [4, 5]. By exploring this kind of complex system through the lens of network science, several structural properties can be better understood, such as the reliability [6, 7], resilience [8, 9], safety [10, 11], and vulnerability [12, 13]. Network science, coupled by a variety of topics like game theory [14, 15, 16], evidential network [17, 18], Bayesian network [19, 20, 21], evidence theory [22, 23], optimization algorithms [24, 25, 26], fuzzy theory [27, 28], and artificial intelligence [29, 30, 31, 32], has allowed us to model multi-disciplinary complex systems using real-world conditions.

Analysis of reliability and vulnerability has always been the focus of research of transportation network performance [33, 34, 35, 36]. In general, research pertaining to network reliability analysis attempts to address this problem from two perspectives. The first one is to identify and measure the characteristic of each individual or the connection between them, such as identifying the importance of nodes for network topology-based cascade models [37, 38]. The other one is to evaluate and explore the property of the entire network and community structure. The resilience

*Corresponding author at: Kang Hao Cheong (kanghao_cheong@sutd.edu.sg)

[39, 40] and vulnerability [41, 42] of communities have been studied to explore the impact of community structure on the construction of transportation networks. For network, researchers also analyzed several properties of real-world network, such as assessing the risk of the electric power system of New York State from the transportation system scenarios [43], optimizing the configuration of logistics service centers before the disaster [44], studying the safety efficiency of the road transportation network [45], and designing a network with the least cost that can meet resilience constraints of the system [46]. It is worth noting that the property of the network (macroscale) may shed light on the property of communities (mesoscale) and individuals (microscale).

Since the maritime logistics network occupies a large proportion of the global trade volume (80%), it has become an indispensable element of transportation network, thus playing an increasingly important role in the world [3]. Buyers' demand for goods is transformed into a comprehensive need for goods that is timely, reliable and cost-efficient [47]. Researchers have started to study the impact of accidents on maritime networks [48]. For example, the vulnerability of global supply chains caused by disruptions in maritime transportation services was studied in the Americas from the perspective of multiplex network [49], the accident risk in the maritime transportation is assessed based on Markov modelling and Markov Chain Monte Carlo simulation [50], the vulnerability of the maritime network was evaluated based on the centrality distribution of ports [51], an optimal resilience model was proposed to manage the residual resilience of ports and routes based on the post-disaster analysis in a maritime transportation network of 23 cities [52], and the delayed maritime transportation of essential goods after earthquake was studied in British Columbia based on the Bayesian network [53].

As discussed above, prior research in the maritime transportation network has primarily focused on one aspect, that is, port or network. However, our proposed model can identify the importance of ports and evaluate the vulnerability of the maritime transportation network at the same time to fill this important gap. Specifically, the importance and connection pattern of each port will be identified from three different aspects at the same time, so as to fully consider the topological characteristic of the network, including (1) neighborhood-based centrality (k-core decomposition), (2) gravity-based centrality, (3) iterative refinement centrality (PageRank). The centrality scores of ports obtained by different measures are then normalized. The vulnerability of the maritime transportation network is explored by considering the normalized centrality score of three measures based on the joint entropy and the multiscale factor. The multiscale factor q can be adjusted to reflect different statistical characteristics of the network. The applicability and performance of this proposed model is demonstrated by the Asia-Europe maritime transportation network and three typical theoretical networks. The relationship between different centrality measures is explored by Pearson correlation coefficient in the experiment. The experimental results suggest that the heterogeneity of the connectivity pattern and the degree of uniformity of the centrality distribution are closely related to the vulnerability of the network. The process of decentralization shows that the impact of the nodes with high centrality score on the vulnerability of the entire network. This proposed vulnerability evaluation approach can be further applied to other types of transportation network. Hence, this proposed model can help individuals, companies, and governments to design the transportation network in the initial stage.

The rest of this paper is organized as follows. Section 2 develops the proposed entropy-based vulnerability measurement model in detail. The numerical experiments are performed in Section 3 through the application of the Asia-Europe maritime transportation network. The conclusions and discussions are given in Section 4.

2. Entropy-based vulnerability evaluation method

In this section, a new method is proposed to evaluate the vulnerability of logistics networks. This proposed approach will consider multiple source of information from different aspects of the network, including neighborhood-based centrality, gravity-based centrality, and iterative refinement centrality. The topological structure information of the logistics network can be fully discovered by these three types of centrality. A vulnerability evaluation model is then applied to fuse these information based on the joint entropy and the multiscale factor.

2.1. Structure of complex networks

For a given complex network $G(N, E)$, N and E represent the set of nodes and edges respectively, $|N|$ and $|E|$ indicate the number of nodes and edges in the networks respectively. The topological structure of the network is given by the adjacency matrix $A_{|N|\times|N|}$, where $A_{ij} = 1$ indicates there is an edge between node i and node j and vice versa.

The shortest path between each pair of nodes can be identified by Dijkstra algorithm and the distance of the shortest path is defined as,

$$d_{ij} = a_{i\eta_1} + a_{\eta_1\eta_2} + ... + a_{\eta_m j}, \tag{1}$$

where $\eta_1, \eta_2, ..., \eta_m$ are IDs of nodes that are on the shortest path between node i and j, and $a_{i\eta_1}, a_{\eta_1\eta_2}, a_{\eta_m j}$ are elements in the adjacency matrix. The degree k_i of node i is then defined as,

$$k_i = \sum_{j \in N} a_{ij}, \tag{2}$$

and it indicates the number of edges that connected with node i.

2.2. Centrality measures

The topological structure information of each node can be described by the centrality. Different types of centrality are considered in our proposed method to discover the characteristic from different aspects, resulting in a more accuracy vulnerability evaluation result. Specifically, (1) the neighborhood-based centrality (k-core decomposition) indicates the position of each node in the network; (2) the gravity-based centrality considers the information of each node and the relationship with other nodes; and (3) the iterative refinement centrality (PageRank) shows the influence of each node based on the influence of its neighbors rather than the number of its neighbors. The definitions of these models are introduced below in detail.

2.2.1. Neighborhood-based centrality

The degree of nodes only consider the number of the nearest neighbors, resulting in many nodes with the same degree. Hence, Kitsak *et al.* [54] argued that the location is much more important than the degree because it indicates whether the node is located in the core part or the periphery of the network. The k-core decomposition [55], one of the most popular neighborhood-based centrality, is applied in our model to show the function of transshipment terminals in the logistics network. In the logistics network, the coreness η_i of isolated nodes ($k_i = 0$) is defined as 0, that is, $\eta_i = 0$. These nodes with $k \leq 1$ are then removed from the network continually until the degree of remaining nodes is lager than 1, and the coreness of these nodes is $\eta_i = 1$. These nodes with larger coreness ($\eta_i = 2, 3, ...$) can be then identified until all nodes are removed from the network. An example of this centrality is given in Figure 1. The k-core decomposition approach can identify whether the seaport is located in the core part or the periphery of the network, so it can better reflect the importance of the port than other neighborhood-based centralities that only consider the number of immediate neighbors. The seaport located in the central position in the logistics network has a higher value of η_i than the seaport in the periphery, resulting in its higher importance.

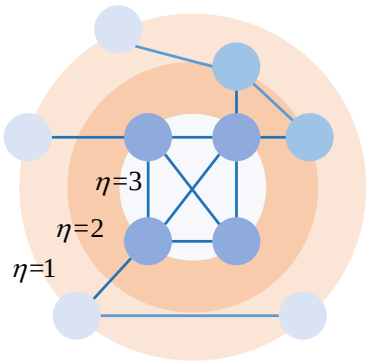


Figure 1: Example of k-core decomposition approach.

2.2.2. *Gravity-based centrality*

Based on the gravity law, each object can attract other objects, thereby causing gravity force. In the network, the mass of objects is represented by the degree of nodes, and the distance between objects is defined by the distance of the shortest path identified by Dijkstra algorithm. Inspired by the formula of the gravity law, the gravity index of each individual [56, 57] can be defined as follows,

$$\delta_i = \sum_{j \in N, j \neq i} \frac{k_i \times k_j}{d_{ij}}, \tag{3}$$

where k_i and d_{ij} are the degree and the shortest distance which have been introduced in Section 2.1. An example of this centrality measure is given in Figure 2. Node j can be all nodes other than node i, indicating the relationship between node i and all other nodes. The gravity model takes into account both the neighbor information and path information, which makes use of more topological information of the network than other classical approaches. According to the definition in Eq. (3), transshipment terminals play a more important role in the logistics network when they have more neighbors (more nodes that can be reached directly) and are closer to other transshipment nodes with higher influential ability, which adopts the formula of the gravity law. For example, the logistics network will be divided into several discontinuous sub-networks due to the unfuntion of these terminals with higher δ_i, resulting in the temporary failure in the network; these terminals with higher δ_i can also take on more roles to avoid greater losses in the logistics network when their neighbor nodes cannot work.

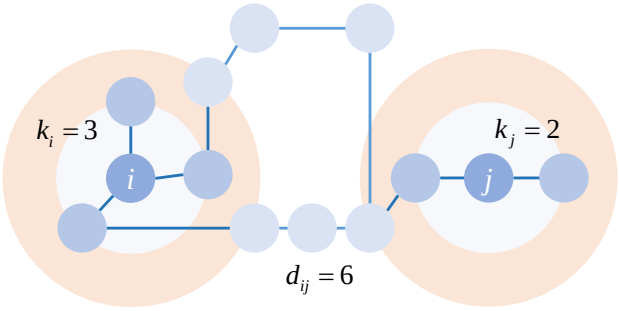


Figure 2: Example of gravity-based centrality.

2.2.3. *Iterative refinement centrality*

The importance of a node not only depends on the number of its neighbor nodes, but also relies on the importance of its neighbor nodes. Hence, PageRank [58], the well-known algorithm to rank websites in Google, is applied as an iterative refinement centrality to explore the degree to which each node is supported by its neighbors. This algorithm considers both the quantity and quality of nodes to identify their importance based on the topological structure of the network through random working. The PageRank value is the same for every nodes $\zeta_i(0)$ at the beginning, and is updated based on the rule below,

$$\zeta_i(t) = s \sum_{j \in N} a_{ji} \frac{\zeta_i(t-1)}{k_j^{out}} + (1-s)\frac{1}{|N|}, \tag{4}$$

where a_{ji} is an element of the adjacency matrix A, k_j^{out} is the out-degree of node i. If the network is an undirected network, each undirected edge will be replaced by two directed edges, rendering the original network to be a directed network. To avoid non-convergence [59], each node will walk to its neighbor nodes with probability s, and walk to a random node (ignoring the structure) with probability $(1-s)$. Eq. (4) will degenerate to the classical form that only considers the network structure when $s = 1$. The importance of each node will be evaluated by the PageRank value when $\zeta_i(t)$ of all nodes become steady. This centrality takes into account both the number and importance of neighbors of each port, thus, the local information is fully applied to identify the importance of each port. In the logistics network, a terminal can get more support from its neighbor terminals when it has a high value of ζ_i, including transshipment and rescue, leading to its higher importance.

2.3. Entropy-based method

In order to measure the vulnerability of the logistics network from the perspective of entropy, the score obtained from each centrality measure needs to be normalized to the interval [0, 1]. The probability distribution of nodes in the network is obtained by,

$$p_i^x = \frac{x_i}{\sum\limits_{i \in N} x_i}, x \in \{\eta, \delta, \varsigma\}, \tag{5}$$

where x_i is the value of node i obtained by different methods, and p_i^x is the normalized score of node i obtained by different methods. Here, x_i can represent the coreness η_i, gravity index δ_i, and PageRank value ς_i. The probability set obtained by each method is given as,

$$P^X = \left\{p_1^x, p_2^x, ..., p_n^x\right\}. \tag{6}$$

Rényi entropy that is a generalized entropy to consider the weights of probabilities is defined as

$$R^X = \frac{\log_2 \sum\limits_{i \in N} \left(p_i^x\right)^q}{(1-q)}. \tag{7}$$

More properties and discussions about Rényi entropy can refer to Ref. [60, 61, 62]. The multiscale approach to evaluate the vulnerability of logistics network is then developed,

$$\psi^X = \left(\frac{R^X}{|E|}\right)^{\frac{1}{|q|}} = \left(\frac{\log_2 \sum\limits_{i \in N} \left(p_i^x\right)^q}{(1-q)\,|E|}\right)^{\frac{1}{|q|}}, \tag{8}$$

where p_i^x is the normalized score of node i obtained by method x, $|E|$ is the number of edges, q is the multiscale factor which can be adjusted based on the topology of network. Unlike only considering the entropy measure, our proposed method takes into account more information of network topology.

2.4. Vulnerability evaluation

The vulnerability evaluated by different measures is given by,

$$\begin{aligned} \psi^\eta &= \left(\tfrac{R^\eta}{|E|}\right)^{\frac{1}{|q|}}, \text{when} P^X = P^\eta, \\ \psi^\delta &= \left(\tfrac{R^\delta}{|E|}\right)^{\frac{1}{|q|}}, \text{when} P^X = P^\delta, \\ \psi^\varsigma &= \left(\tfrac{R^\varsigma}{|E|}\right)^{\frac{1}{|q|}}, \text{when} P^X = P^\varsigma, \end{aligned} \tag{9}$$

where ψ^η, ψ^δ, ψ^ς are the vulnerability degree of the logistics network obtained by the normalized coreness score, normalized gravity score, and normalized PageRank score. When $p_{ijk}^{\eta\delta\varsigma}$ represents the joint probability distribution of P^η, P^δ, and P^ς, the joint entropy $\bar{\psi}$ of these distributions is defined by,

$$\bar{\psi} = \psi^{\eta\delta\varsigma} = \left(\frac{R^{\eta\delta\varsigma}}{|E|}\right)^{\frac{1}{|q|}} = \left(\frac{\log_2 \sum\limits_{i \in N} \sum\limits_{j \in N} \sum\limits_{k \in N} \left(p_{ijk}^{\eta\delta\varsigma}\right)^q}{(1-q)\,|E|}\right)^{\frac{1}{|q|}}. \tag{10}$$

In addition, the joint entropy is usually less than or equal to the sum of individual entropies, that is,

$$\psi^{\eta\delta\varsigma} \leq \psi^\eta + \psi^\delta + \psi^\varsigma. \tag{11}$$

In this paper, three centrality measures are considered simultaneously to evaluate the vulnerability of the logistics network. Since P^η, P^δ, and P^ς are mutually independent, the joint entropy $\bar{\psi}$ can be also obtained by,

$$\bar{\psi} = \psi^{\eta\delta\varsigma} = \psi^\eta + \psi^\delta + \psi^\varsigma. \tag{12}$$

Obviously, entropy will reach the maximum value when the probability set is uniformly distributed, that is,

$$p_i^x = \frac{1}{|N|}, x \in \{\eta, \delta, \varsigma\}, i \in N. \tag{13}$$

Hence, the maximum entropy is defined as,

$$\begin{aligned} \psi_{max}^X &= \left(\frac{\log_2 \sum_{i \in N} \left(\frac{1}{|N|}\right)^q}{(1-q)|E|} \right)^{\frac{1}{|q|}} = \left(\frac{\log_2 \left(\frac{1}{|N|}\right)^{q-1}}{(1-q)|E|} \right)^{\frac{1}{|q|}} \\ &= \left(\frac{\log_2 |N|}{|E|} \right)^{\frac{1}{|q|}}, X \in \{\eta, \delta, \varsigma\}, \end{aligned} \tag{14}$$

and the maximum joint entropy is given by,

$$\psi_{max}^{\eta\delta\varsigma} = 3 \times \left(\frac{\log_2 |N|}{|E|} \right)^{\frac{1}{|q|}}. \tag{15}$$

Hence, the vulnerability of the logistic network that considers several centrality measures is defined as,

$$\nu = 1 - \frac{\bar{\psi}}{\psi_{max}^{\eta\delta\varsigma}} = 1 - \frac{\psi^{\eta\delta\varsigma}}{\psi_{max}^{\eta\delta\varsigma}}, \tag{16}$$

which is related to the difference between the joint entropy and its maximum entropy. Our proposed vulnerability evaluation approach has the following properties,

1) ν is a dimensionless value in $[0, 1)$;

2) The logistics network is more vulnerable with higher value of ν;

3) ν equals to 0 only when all nodes have the same score obtained by different centrality measures (fully connected network);

4) ν is high when the property (such as connectivity) of nodes in the network is extremely unbalanced;

5) The mutilscale factor q can be adjusted according to the type of network;

6) This model can easily be generalized to consider more information achieve better outcomes if users need.

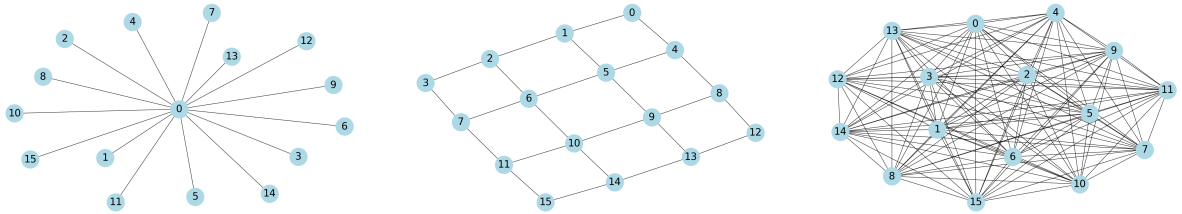
In our proposed method, ν can measure the degree of uniformity of the distribution in the logistics network, which compares the joint entropy and its maximum entropy. Hence, the impact of the failure of each node on the performance of the entire network can be reflected by this index.

In this paper, $q = 2$ is taken as an example to illustrate the applicability and effectiveness of this proposed method. Rényi entropy will degenerate to the Collision entropy when $q = 2$ that is sensitive to the hub transshipment terminals due to the power of probabilities. In addition, it can measure the impact of the centrality of each node on the vulnerability of the network, thereby showing the effect of the heterogeneity.

2.5. *Illustrative examples*

Three simple networks with different characteristics are first used as examples to illustrate our method. All of them are closely linked to the real-world transportation network. The topological structure of these networks is shown in Figure 3. The star network (Figure 3(a)), lattice network (Figure 3(b)), and fully connected network (Figure 3(c)) represent the hub-and-spoke network, grid road network, and point-to-point transit network in the real-world, respectively. The size is the same in three networks to avoid the its impact on the vulnerability.

ψ^X for $X \in \{\eta, \delta, \varsigma\}$ are given in Table 1 when the size of networks is $|N| = 9$. The vulnerability indexes ν of three networks when $|N| = 9, 16, 36, 64$ are also given in Table 1. The results show that the fully connected network has the lowest vulnerability ($\nu = 0$) in three networks, followed by the lattice network ($\nu = 0.0114$), and the star network has the highest vulnerability ($\nu = 0.0971$). It is the same as the realistic situation because (1) the highly



(a) Star network (b) Lattice network (c) Fully connected network

Figure 3: Three contrasting networks with the same number of nodes.

concentrated center node (like node 0 in Figure 3(a)) render the star network as the most vulnerable network, (2) the lower vulnerability of the lattice network is caused by its relatively homogeneous structure, (3) the fully connected network is the least vulnerable as each node can reach the entire network via an edge. Hence, it indicates that the homogeneous distribution of the topology of the fully connected network renders it to be the most robust network ($\nu = 0$). When the size of network $|N|$ increases, the fully connected network is always the least vulnerable network ($\nu = 0$) due to its homogeneous distribution. The lattice network becomes less vulnerable when the size is larger because there will be more nodes with the same centrality score. However, the star network will be more vulnerable ($\nu = 0.0971, 0.1629, 0.2128, 0.2418$) when the size increases due to the more centralized center node.

Table 1: Vulnerability of three theoretical networks.

Network	$\|N\| = 9$				$\|N\| = 16$	$\|N\| = 36$	$\|N\| = 64$
	ψ^η	ψ^δ	ψ^ς	ν	ν	ν	ν
Star network	0.6295	0.5291	0.5032	0.0971	0.1629	0.2128	0.2418
Lattice network	0.5140	0.5011	0.5092	0.0114	0.0090	0.0054	0.0038
Fully connected network	0.2967	0.2967	0.2967	0.0000	0.0000	0.0000	0.0000

Before evaluating the vulnerability of networks by this proposed approach, the impact of the multiscale factor q is studied. $q = 2, 3, 5$ are applied to show the impact on the vulnerability ν of the star network (S), lattice network (L), and fully connected network (C). The vulnerability of three types of networks with different sizes $|N|$ and multiscale factors q is shown in Figure 4. Under different values of q, the star network is always the most vulnerable (highest value of ν), followed by the lattice network, and the fully connected network is the most stable ($\nu \equiv 0$ regardless of the value of q and $|N|$). It means that the vulnerability ν of networks is robust to changes in q. In addition, the star network becomes more vulnerable as the size increases due to its highly concentrated center node, whereas the lattice network becomes more stable as the size increases.

Two similar networks are applied to show the effectiveness of this proposed approach by comparing with classical methods. The structure of the two networks is shown in Figure 5(a), including the bat network G_1 and umbrella network G_2. The only difference between two networks is the edge $\{\{1,3\},\{4,6\}\}$ in G_1 and $\{\{1,6\},\{3,4\}\}$ in G_2. G_1 is more vulnerable than G_2 because the attack on node 7 (red node in Figure 5(a)) causes G_1 to be divided into 3 disconnected sub-networks, while G_2 only becomes 2 components. Therefore, the vulnerability of two networks is different. However, these methods based on degree centrality and eigenvector centrality cannot be applied to measure the vulnerability of two networks due to the same degree distributions and eigenvectors with maximal/minimal eigenvalues, such as Refs. [63, 64]. The average edge betweenness [65] that can measure the vulnerability of networks is defined below,

$$b(G) = \frac{1}{|E|}\sum_{l\in E} b_l \tag{17}$$

where E and $|E|$ represent the set and number of edges respectively, and b_l is the edge betweenness of edge l [66]. However, $b(G_1) = b(G_2) = 43/13$ indicates the identical vulnerability of the two networks. In addition, the vulnerability of the two networks is the same measured by the maximum efficiency reduction after removing the edge

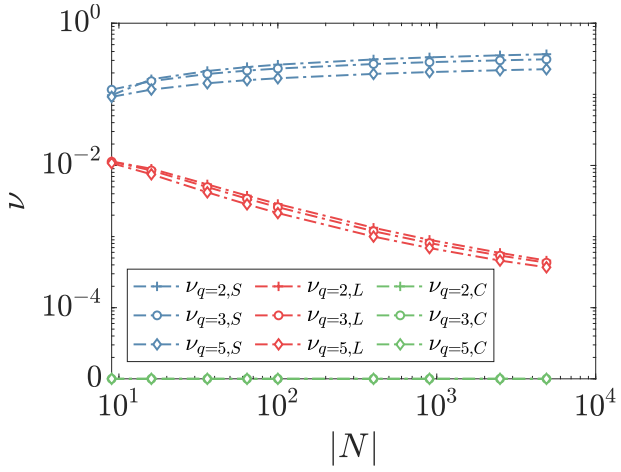
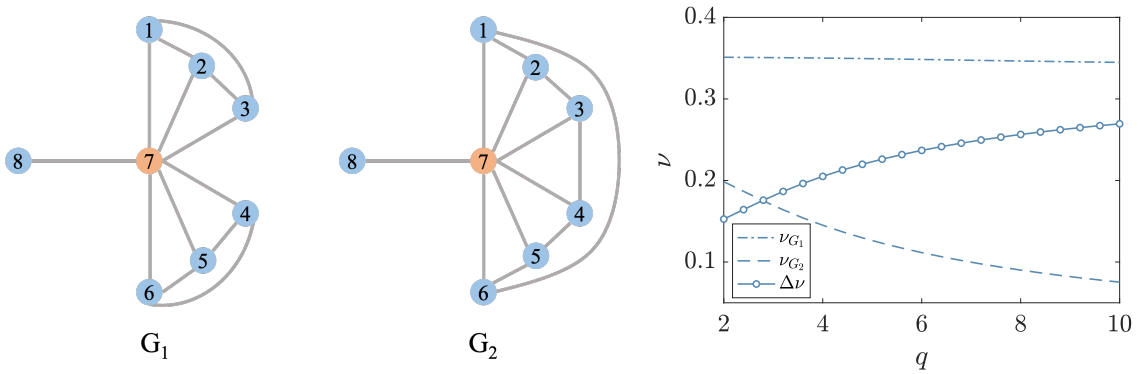


Figure 4: Vulnerability of three types of networks under different values of $|N|$ and q.

$(\nu(G_1) = \nu(G_2) = 0.1951)$ [67]. All of these methods have failed to distinguish the vulnerability of the two networks. However, our proposed method can clearly show the difference $(\nu(G_1) \neq \nu(G_2)$ when $q \in [2, 10])$ in Figure 5(b), and the difference between the vulnerability of two networks $\Delta\nu = \nu(G_1) - \nu(G_2)$ becomes larger as q increases. Therefore, compared with these methods, our proposed method can effectively measure the vulnerability of networks based on the structure.



(a) Structure of networks

(b) Vulnerability of networks

Figure 5: The bat network G_1 and umbrella network G_2, including (a) the structure and (b) the vulnerability of two networks. In this experiment, the gravity-based centrality is replaced by the betweenness centrality to illustrate that our proposed method can effectively measure the vulnerability of networks based on different centrality measures.

3. Experiments

The real-world maritime network is applied in this paper to validate the effectiveness and applicability of our proposed model. Due to the rise of global trade, maritime networks have become more important as a typical representative of transportation networks and global supply chain networks. However, the relationship between the vulnerability of the maritime transportation network and accidents has rarely been studied [68]. Hence, exploring the impact of topological structure of the network on its vulnerability can greatly contribute to the improvement and development of the global supply chain network.

3.1. Data

The Asia-Europe maritime logistics network [68] that is the busiest and most important maritime network in the world is used as a case to explore in this paper. This maritime transportation network (Figure 6) contains 54 seaports and 112 routes all over the world, where the name and ID of seaports are given in Table 2. The node and edge in the network represent the seaport and route in the transportation system respectively. This network is a undirected and unweighted network but it is sufficient to explore the impact of structure information of on the vulnerability of the logistics network.

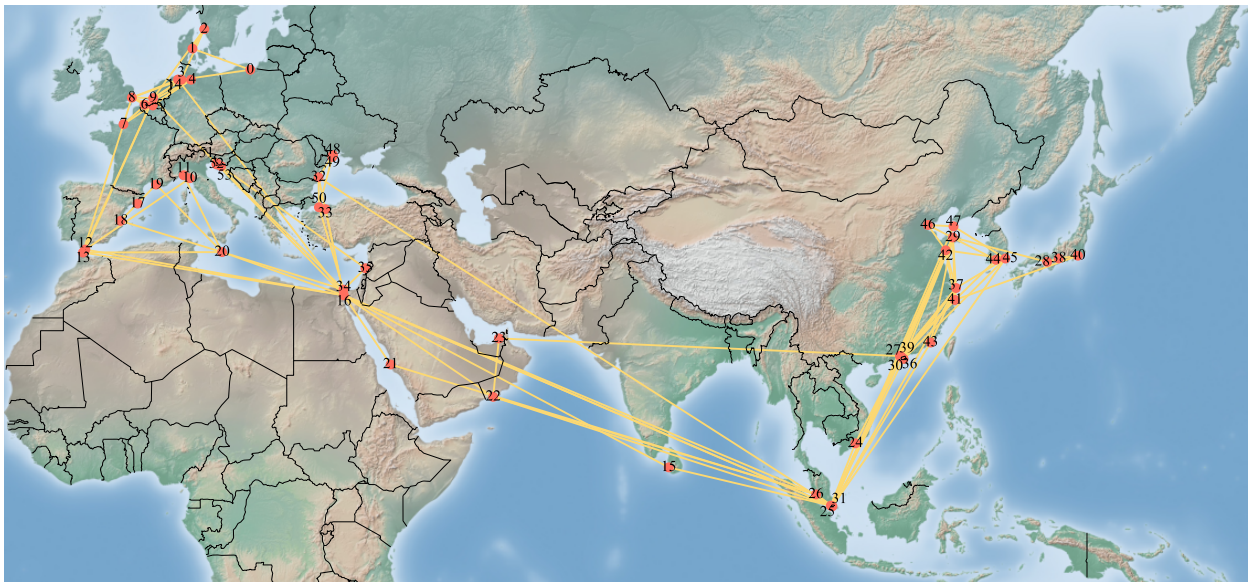


Figure 6: The structure of the maritime transportation network.

Table 2: ID and name of seaports in the Asia-Europe maritime transportation network.

ID	Port	ID	Port	ID	Port
0	Gdansk	18	Valencia	36	Chiwan
1	Aarhus	19	Fos-sur-Mer	37	Shanghai
2	Gothenhurg	20	Marsaxlokk	38	Nagoya
3	Bremerhaven	21	Jeddah	39	Nansha
4	Hamburg	22	Salalah	40	Yokohama
5	Antwerp	23	Jebel Ali	41	Ningbo
6	Zeebrugge	24	Vung Tao	42	Qingdao
7	Le Harve	25	Tanjung Pelepas	43	Xiamen
8	Felixstowe	26	Port Klang	44	Kwangyang
9	Rotterdam	27	Nansha New Port	45	Busan
10	La Spezia	28	Kobe	46	Xingang
11	Genoa	29	Yantain	47	Dalian
12	Algeciras	30	Hong Kong	48	Odessa
13	Port Tangiers	31	Singapore	49	Ilyichevsk
14	Whihelmshaven	32	Constantza	50	Ambarli
15	Colombo	33	Izmit Korfezi	51	Trieste
16	Suez Canal	34	Port Said	52	Koper
17	Barcelona	35	Beirut	53	Rijeka

3.2. Port importance identification

From this subsection, the vulnerability of the logistics network will be studied step by step. Firstly, the importance and influential ability of each seaport will be identified by three centrality methods based on different topology

information (introduced in Section 2.2). The normalized score and rank of each port obtained by k-core decomposition approach, gravity-based centrality, and PageRank centrality are shown in Table 3, 4, and 5, respectively. Here, ports with duplicate scores are assigned the same rank. Ports with high scores are identified as important ports in the maritime transportation network due to the characteristics of each centrality measure (Section 2.2). Observed from Table 3, there are many nodes with the same score η_i and rank so we cannot distinguish between the differences of these nodes and their impact on the vulnerability of the network. However, this method can easily identify the center seaport in the maritime network. The outcome is caused by the inherent characteristic of this k-core decomposition approach. The normalized score given by gravity-based centrality (Table 4) and PageRank centrality (Table 5) can be used to identify the importance of each port clearly, and there are almost no nodes with the same score (apart from node 18 and 19 as well as node 52 and 53). The score of each seaport is then visualized on the network (Figure 7). Here, the size of nodes represents the score obtained by different centrality methods, where the node with a higher centrality score has a larger size, thereby indicating the importance of ports in the maritime network. Except for the similar size of nodes in Figure 7(a), the size of nodes is different in Figure 7(b) and 7(c), reflecting the importance of nodes. We can find that nodes (ports) near the center of the network are usually of higher importance (Figure 7).

Table 3: Normalized score η_i obtained by k-core decomposition approach.

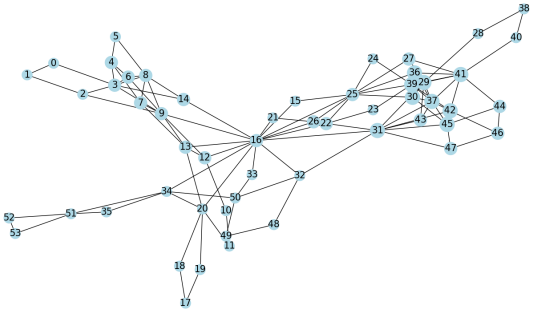
ID	η_i	Rank	ID	η_i	Rank	ID	η_i	Rank
0	1.389×10^{-2}	28	18	1.389×10^{-2}	28	36	2.778×10^{-2}	1
1	1.389×10^{-2}	28	19	1.389×10^{-2}	28	37	2.778×10^{-2}	1
2	1.389×10^{-2}	28	20	1.389×10^{-2}	28	38	1.389×10^{-2}	28
3	2.083×10^{-2}	10	21	1.389×10^{-2}	28	39	2.778×10^{-2}	1
4	2.083×10^{-2}	10	22	2.083×10^{-2}	10	40	1.389×10^{-2}	28
5	1.389×10^{-2}	28	23	1.389×10^{-2}	28	41	2.778×10^{-2}	1
6	2.083×10^{-2}	10	24	1.389×10^{-2}	28	42	2.778×10^{-2}	1
7	2.083×10^{-2}	10	25	2.083×10^{-2}	10	43	2.083×10^{-2}	10
8	2.083×10^{-2}	10	26	2.083×10^{-2}	10	44	2.083×10^{-2}	10
9	2.083×10^{-2}	10	27	2.083×10^{-2}	10	45	2.778×10^{-2}	1
10	1.389×10^{-2}	28	28	1.389×10^{-2}	28	46	2.083×10^{-2}	10
11	1.389×10^{-2}	28	29	2.778×10^{-2}	1	47	2.083×10^{-2}	10
12	2.083×10^{-2}	10	30	2.778×10^{-2}	1	48	1.389×10^{-2}	28
13	2.083×10^{-2}	10	31	2.778×10^{-2}	1	49	1.389×10^{-2}	28
14	2.083×10^{-2}	10	32	1.389×10^{-2}	28	50	1.389×10^{-2}	28
15	1.389×10^{-2}	28	33	1.389×10^{-2}	28	51	1.389×10^{-2}	28
16	2.083×10^{-2}	10	34	1.389×10^{-2}	28	52	1.389×10^{-2}	28
17	1.389×10^{-2}	28	35	1.389×10^{-2}	28	53	1.389×10^{-2}	28

Table 4: Normalized score δ_i obtained by gravity-based centrality.

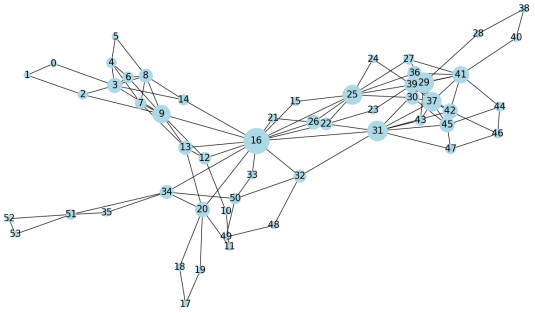
ID	δ_i	Rank	ID	δ_i	Rank	ID	δ_i	Rank
0	5.969×10^{-3}	48	18	6.637×10^{-3}	44	36	2.415×10^{-2}	15
1	5.511×10^{-3}	51	19	6.637×10^{-3}	44	37	4.682×10^{-2}	5
2	1.127×10^{-2}	32	20	2.789×10^{-2}	10	38	5.565×10^{-3}	50
3	2.785×10^{-2}	11	21	8.519×10^{-3}	36	39	2.609×10^{-2}	12
4	1.292×10^{-2}	29	22	1.915×10^{-2}	20	40	6.428×10^{-3}	46
5	5.984×10^{-3}	47	23	7.760×10^{-3}	38	41	3.558×10^{-2}	7
6	1.567×10^{-2}	23	24	8.218×10^{-3}	37	42	2.878×10^{-2}	8
7	1.572×10^{-2}	22	25	4.835×10^{-2}	4	43	1.368×10^{-2}	26
8	2.364×10^{-2}	17	26	2.566×10^{-2}	13	44	1.137×10^{-2}	31
9	4.061×10^{-2}	6	27	1.353×10^{-2}	27	45	2.791×10^{-2}	9
10	6.653×10^{-3}	43	28	7.346×10^{-3}	39	46	1.031×10^{-2}	33
11	6.698×10^{-3}	41	29	5.240×10^{-2}	2	47	1.228×10^{-2}	30
12	1.878×10^{-2}	21	30	2.396×10^{-2}	16	48	6.727×10^{-3}	40
13	2.450×10^{-2}	14	31	5.175×10^{-2}	3	49	5.603×10^{-3}	49
14	1.411×10^{-2}	25	32	1.955×10^{-2}	19	50	1.479×10^{-2}	24
15	9.225×10^{-3}	34	33	8.580×10^{-3}	35	51	1.333×10^{-2}	28
16	8.424×10^{-2}	1	34	2.321×10^{-2}	18	52	5.173×10^{-3}	52
17	5.049×10^{-3}	54	35	6.665×10^{-3}	42	53	5.173×10^{-3}	52

3.3. Centrality comparison

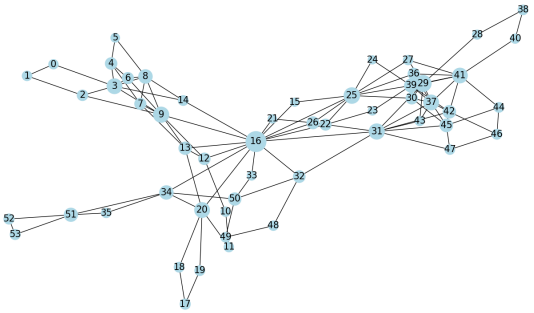
The three centrality measures consider different structure information in the network and give different outcome, so we compare them in this subsection in detail. The normalized score and distribution of three centrality measures are shown in Figure 8. Due to the large number of duplicated scores obtained by the k-core decomposition, δ and ς are mainly analyzed in this section. Node 16 has the highest δ_{16} and ς_{16} at the same time, indicating node 16 (Suez



(a) Maritime network based on η_i



(b) Maritime network based on δ_i



(c) Maritime network based on ς_i

Figure 7: Maritime networks, where the size of the node represents the importance of the port.

Table 5: Normalized score ς_i obtained by PageRank centrality.

ID	ς_i	Rank	ID	ς_i	Rank	ID	ς_i	Rank
0	1.21887×10^{-2}	45	18	1.35037×10^{-2}	33	36	1.79703×10^{-2}	22
1	1.26710×10^{-2}	41	19	1.35037×10^{-2}	34	37	3.01761×10^{-2}	6
2	1.53439×10^{-2}	27	20	2.99825×10^{-2}	7	38	1.32040×10^{-2}	36
3	2.98963×10^{-2}	8	21	9.96643×10^{-3}	52	39	2.30251×10^{-2}	13
4	1.83048×10^{-2}	20	22	1.69661×10^{-2}	26	40	1.19527×10^{-2}	47
5	1.07074×10^{-2}	50	23	1.01668×10^{-2}	51	41	2.96772×10^{-2}	9
6	1.72793×10^{-2}	24	24	9.70668×10^{-3}	54	42	2.18204×10^{-2}	15
7	1.72279×10^{-2}	25	25	3.29975×10^{-2}	3	43	1.20239×10^{-2}	46
8	2.50705×10^{-2}	10	26	1.99175×10^{-2}	18	44	1.32433×10^{-2}	35
9	3.15519×10^{-2}	5	27	1.24174×10^{-2}	44	45	2.20159×10^{-2}	14
10	1.24273×10^{-2}	43	28	1.17981×10^{-2}	48	46	1.36380×10^{-2}	31
11	1.26717×10^{-2}	39	29	3.51642×10^{-2}	2	47	1.31006×10^{-2}	37
12	1.82708×10^{-2}	21	30	1.79425×10^{-2}	23	48	1.26712×10^{-2}	40
13	2.10320×10^{-2}	16	31	3.17821×10^{-2}	4	49	1.29771×10^{-2}	38
14	1.35391×10^{-2}	32	32	1.88780×10^{-2}	19	50	2.10287×10^{-2}	17
15	9.71269×10^{-3}	53	33	1.09851×10^{-2}	49	51	2.39902×10^{-2}	12
16	5.38294×10^{-2}	1	34	2.47668×10^{-2}	11	52	1.41706×10^{-2}	29
17	1.45088×10^{-2}	28	35	1.24651×10^{-2}	42	53	1.41706×10^{-2}	29

Canal) is the most important seaport in the global logistics network, which is consistent with intuition. All (shortest) maritime transport between Asia and Europe needs to pass through Suez Canal. η_{16} is not the largest as the k-core decomposition approach always identify the center node as the most important one, but it is usually the most central node that has the highest importance in the maritime network. Node 29 (Yantain) is identified as the most important seaport (η_{29}) by the k-core decomposition approach, and it is the second most important node identified by the other two centrality measures (δ_{29} and ς_{29}). Three centrality methods reached a consensus at this port because it locates in the center of East Asia and undertakes the transshipment of a large number of goods in this region. Node 25 (Tanjung Pelepas) and node 31 (Singapore) are also ranked very high (δ and ς) because they are in the key area of the Straits of Malacca and play an important role in Southeast Asia. Node 9 (Rotterdam) is then identified as the important seaport in the logistics network by δ and ς at the same time because Rotterdam has been Europe's largest seaport for a long time. Node 37 (Shanghai), and node 41 (Ningbo) are identified as important nodes by η, δ, and ς at the same time, because it undertakes the sending and receiving of goods in the fastest growing and richest regions of China and even East Asia – the Yangtze Delta. Node 42 (Qingdao) and Node 45 (Busan) are two important seaports in the logistics network identified by η and δ at the same time. There are also some unimportant nodes that can be recognized by different centrality methods at the same time, such as node 17 (Barcelona) and node 24 (Vung Tao), because they are near other important seaports and have few routes. Figure 8 show that the distribution of η is the most uniform, followed by ς, and the distribution of δ is the most uneven.

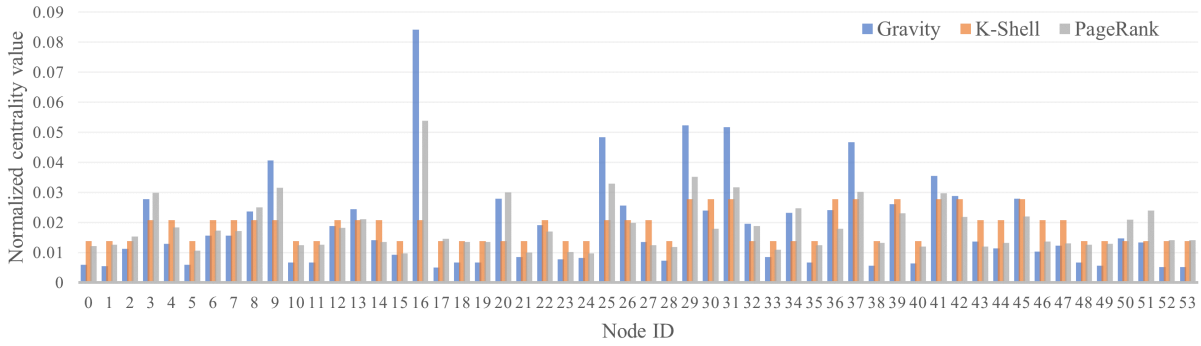


Figure 8: Normalized score obtained by different centrality methods, including the gravity-based centrality (blue), K-core decomposition approach (orange), and PageRank (gray).

The Pearson correlation coefficient r is then applied to measure the correlation between the distribution of every

two centrality measures. r is defined as follows,

$$r = \frac{\sum (x - m_x)\left(y - m_y\right)}{\sqrt{\sum (x - m_x)^2 \sum \left(y - m_y\right)^2}}, \tag{18}$$

where m_x and m_y are the mean of x and y, respectively. Two centrality measures will give the same rank when $r = 1$ and give totally different ranks when $r = -1$. The values of r are given in Table 6. It shows that δ and ς are closely related ($r = 0.9459$) because they can give each nodes a unique score. However, the k-core decomposition approach gives many nodes with the same η, which is difficult to evaluate the importance of each port and leads to irrelevance to the other methods. Different methods will give a different evaluation of the importance of nodes as they consider different kinds of topology information [69].

Table 6: The Pearson correlation coefficient r between the distribution of every pair of centrality measures.

Pearson r	δ	η	ς
δ	1.0000	0.6413	0.9450
η	0.6413	1.0000	0.5080
ς	0.9450	0.5080	1.0000

3.4. Vulnerability of the maritime network

In order to evaluate the property of maritime network reasonably, more topology information should be considered in the process. Accurate results cannot be obtained by only considering single information because of insufficient understanding of network information. This paper takes into account the k-core decomposition approach, gravity-based centrality, and PageRank centrality to measure the vulnerability of the maritime logistics network. Compared with the voting method proposed by Liu *et al.* [68], this proposed method is completely objective and there is no subjective deception and other similar behaviors. In addition, more topology information is considered in this proposed than Refs. [51] (multiscale factor q) and [65] (centrality measures). Hence, this proposed model will measure the vulnerability of maritime networks more reasonably. Given the distribution of different centrality measure, the vulnerability of the maritime logistics network is measured by Eqs. (8), (12), and (16). The results of the vulnerability of this network are shown in Table 7. The uniform distributions of η and ς cause the relatively low heterogeneity, resulting the high values of ψ^{η} and ψ^{ς}. However, the distribution of δ is uneven (Figures 7(b) and 8), thus leading to the low value of ψ^{δ}. Hence, the uniformity degree of the distribution of the socre obtained by centrality measures is related to the vulnerability of the entire network. The vulnerability index of the maritime logistics network is $\nu = 0.0342$ (Table 7).

Table 7: The vulnerability of the maritime network.

	ψ^{η}	ψ^{δ}	ψ^{ς}	ν
Maritime network	0.2245	0.2110	0.2212	0.0342

These highly central seaports (with large values of centrality socre) may create further potential crises, thereby increasing the vulnerability of the global maritime transportation network [70]. Failure or accident of this kind of port will lead to a decline in the overall performance of the global maritime transportation network, including transportation capacity, transportation time, and transportation distance. The centralized structure (centralization of network performance control) makes the network structure prone to large-scale cascading failures. This proposed model can evaluate the heterogeneity of the connectivity pattern of the logistics network, thereby indicating the impact of every seaports on the transportation network. In addition, it suggests that the process of decentralization can increase the robust of the transportation network by reducing the heterogeneity of the entire network. Hence, these ports that are recognized by all centrality methods as high centrality score should be tested for their impact on the vulnerability of the entire maritime network, including node 16 (Suez Canal), node 29 (Yantain), node 25 (Tanhung Pelepas), and node 9 (Rotterdam). The process of decentralization is achieved by replacing the centrality score port with the mean value of the corresponding set [51]. This means that a large number of routes associated with these selected ports

will be temporarily adjusted (added or removed) to reduce the centralization of the maritime network in practice. The reduction of these high centrality scores will illustrate the effect of the heterogeneity on the network vulnerability from a quantitative perspective. The process and corresponding ν are given in Table 8. As more ports are replaced by new centrality score, the maritime network will become more reliable (lower ν). At the same time, the rate of vulnerability reduction will also slow down (lower $\Delta\nu$), indicating that the implementation of the decentralization process in the initial stage is more effective. Hence, these ports with high centrality scores are important for improving the reliability of a complex system like the Asia-Europe maritime transportation network.

Table 8: The process of decentralization and corresponding ν.

Scenario	Node	ν	$\Delta\nu$=$\nu(S_i) - \nu(S_{i-1})$
S_0	—	0.0342	—
S_1	16	0.0182	-0.0160
S_2	16,29	0.0109	-0.0073
S_3	16,29,25	0.0051	-0.0059
S_4	16,29,25,9	0.0006	-0.0045

Different centrality measures are further studied in this proposed approach. When replacing the gravity-based centrality with the betweenness centrality, the vulnerability of the maritime network under different scenarios $\hat{S}$ in the decentralization is shown in Table 9. It can be found that the maritime network continues to become more reliable in the process ($\Delta\nu < 0$) and the implementation of the decentralization process is more effective in the initial stage ($\left|\nu\left(\hat{S}_1\right) - \nu\left(\hat{S}_0\right)\right|$ is the largest). When replacing the gravity-based centrality and coreness centrality with the betweenness centrality and degree centrality at the same time, the vulnerability of the maritime network under different scenarios $\tilde{S}$ is also shown in Table 9. In this case, the same conclusion can be obtained, that is, $\Delta\nu < 0$ and $\left|\nu\left(\tilde{S}_1\right) - \nu\left(\tilde{S}_0\right)\right|$ is the largest. Therefore, the maritime becomes more reliable in the process of decentralization regardless of the selection of centrality measures, indicating that our proposed approach is robust to different centrality measures.

Table 9: The vulnerability ν of maritime time during the process of decentralization when different centrality measures are applied.

Scenario	Node	ν	$\Delta\nu$
$\hat{S}_0$	—	0.0894	—
$\hat{S}_1$	16	0.0365	-0.0530
$\hat{S}_2$	16,29	0.0316	-0.0048
$\hat{S}_3$	16,29,25	0.0240	-0.0077
$\hat{S}_4$	16,29,25,9	0.0134	-0.0105
$\tilde{S}_0$	—	0.1005	—
$\tilde{S}_1$	16	0.0413	-0.0592
$\tilde{S}_2$	16,29	0.0341	-0.0072
$\tilde{S}_3$	16,29,25	0.0239	-0.0101
$\tilde{S}_4$	16,29,25,9	0.0115	-0.0124

4. Conclusions

Due to the development of global trade and the progress of globalization, maritime network performance analysis has become an important topic of immense interest. An original and novel network vulnerability index has been proposed in this paper to study the vulnerability in accidents [71]. Our proposed method aims to close some critical gaps in existing methods, such as inadequate consideration of network topology information [65], neglecting the physical (multiscale) factor [51], and the limitations of network-scale measurement [72, 73]. Different from existing models, the importance of ports is measure by three important centrality measures, including k-core decomposition approach, gravity-based centrality, and PageRank centrality. Several kinds of network topology information can be

considered in this proposed model simultaneously. The centrality score of ports is then normalized to study its impact on the vulnerability of the network by joint entropy and the multiscale factor. According to the experiment network and purpose, the multiscale factor q can be adjusted to achieve more accurate measurement. $q = 2$ is taken in this paper to study the effect of these hub transshipment terminals in the maritime network. The vulnerability of the maritime network can be measured by the difference between the joint entropy and its maximum entropy. This proposed vulnerability index ν can measure the heterogeneity of the connectivity pattern and the degree of uniformity of the centrality distribution, thereby showing the effect of the failure of individual node on the performance (vulnerability) of the entire network.

The Asia-Europe maritime transportation network [68] is applied as a test example to validate the applicability of our proposed model in Section 3. The importance of ports is first studied by three centrality measures. The results show that the k-core decomposition approach give several ports with the same score while the other two measures will not. The relationship between the three centrality measures is also discussed in detail, such as analysis of representative ports and Pearson correlation coefficient r. The vulnerability index ν of the original maritime network and corresponding index during the decentralization process are determined, thereby illustrating the importance of these ports with high centrality scores to reduce the vulnerability of the network. It is worth pointing out that our proposed model can be applied not only to maritime transportation networks, but also to other transportation networks in different contexts (high scalability). Transportation between individuals is one of the most important factors to measure the vulnerability of the transportation network, such as airlines in air transport networks, tracks in rail networks, and roads in highway networks. Although manifestations of connections are different, they can be regarded as edges between nodes in all types of transportation networks. Our proposed method can fully take into account the connectivity of networks through different centrality measures, thus can be used in a variety of transportation networks. In addition, this model can be used to help individuals, companies, and governments in the early logistics network design.

Acknowledgment

This work is supported by the Singapore University of Technology and Design (SRG SCI 2019 142).

Conflict of Interest

The authors declare no conflict of interest.

References

[1] V. Colizza, A. Barrat, M. Barthélemy, and A. Vespignani, "The role of the airline transportation network in the prediction and predictability of global epidemics," *Proceedings of the National Academy of Sciences*, vol. 103, no. 7, pp. 2015–2020, 2006.

[2] M. Diao, H. Kong, and J. Zhao, "Impacts of transportation network companies on urban mobility," *Nature Sustainability*, vol. 4, no. 6, pp. 494–500, 2021.

[3] M. Xu, Q. Pan, A. Muscoloni, H. Xia, and C. V. Cannistraci, "Modular gateway-ness connectivity and structural core organization in maritime network science," *Nature Communications*, vol. 11, no. 1, pp. 1–15, 2020.

[4] J. Wang and M. Xie, "Modeling and monitoring unweighted networks with directed interactions," *IISE Transactions*, vol. 53, no. 1, pp. 116–130, 2021.

[5] T. Xiahou, Z. Zeng, Y. Liu, and H.-Z. Huang, "Measuring conflicts of multisource imprecise information in multistate system reliability assessment," *IEEE Transactions on Reliability*, 2021.

[6] S. Jiang and Y.-F. Li, "Dynamic reliability assessment of multi-cracked structure under fatigue loading via multi-state physics model," *Reliability Engineering & System Safety*, vol. 213, p. 107664, 2021.

[7] P. Zhang, M. Xie, and X. Zhu, "Exploiting structural similarity in network reliability analysis using graph learning," *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, p. 1748006X211009329, 2021.

[8] U. Alibrandi and K. M. Mosalam, "A decision support tool for sustainable and resilient building design," in *Risk and Reliability Analysis: Theory and applications*, pp. 509–536, Springer, 2017.

[9] T. Wen and K. H. Cheong, "The fractal dimension of complex networks: A review," *Information Fusion*, vol. 73, pp. 87–102, 2021.

[10] Z. Liu, Y. Deng, Y. Zhang, Z. Ding, and X. He, "Safety assessment of dynamic systems: An evidential group interaction-based fusion design," *IEEE Transactions on Instrumentation and Measurement*, vol. 70, pp. 1–14, 2021.

[11] S. Gao and Y. Deng, "An evidential evaluation of nuclear safeguards," *International Journal of Distributed Sensor Networks*, vol. 15, no. 12, p. 1550147719894550, 2019.

[12] Y. Liu, Q. Liu, C. Xie, and F. Wei, "Reliability assessment for multi-state systems with state transition dependency," *Reliability Engineering & System Safety*, vol. 188, pp. 276 – 288, 2019.

[13] X. Su, S. Mahadevan, P. Xu, and Y. Deng, "Inclusion of task dependence in human reliability analysis," *Reliability Engineering & System Safety*, vol. 128, pp. 41–55, 2014.
[14] C. Shao and Y.-F. Li, "Multistage attack–defense graph game analysis for protection resources allocation optimization against cyber attacks considering rationality evolution," *Risk Analysis*, 2021.
[15] T. Wen, E. V. Koonin, and K. H. Cheong, "An alternating active-dormitive strategy enables disadvantaged prey to outcompete the perennially active prey through parrondo's paradox," *BMC Biology*, vol. 19, no. 1, p. 168, 2021.
[16] S.-Z. Liu, C.-W. Shao, Y.-F. Li, and Z. Yang, "Game attack-defense graph approach for modeling and analysis of cyberattacks and defenses in local metering system," *IEEE Transactions on Automation Science and Engineering*, 2021.
[17] L. Zuo, T. Xiahou, and Y. Liu, "Reliability assessment of systems subject to interval-valued probabilistic common cause failure by evidential networks," *Journal of Intelligent & Fuzzy Systems*, vol. 36, no. 4, pp. 3711–3723, 2019.
[18] L. Zuo, T. Xiahou, and Y. Liu, "Evidential network-based failure analysis for systems suffering common cause failure and model parameter uncertainty," *Proceedings of the Institution of Mechanical Engineers, Part C: Journal of Mechanical Engineering Science*, vol. 233, no. 6, pp. 2225–2235, 2019.
[19] D. Zhang, Q. Liu, H. Yan, and M. Xie, "A matrix analytic approach for bayesian network modeling and inference of a manufacturing system," *Journal of Manufacturing Systems*, vol. 60, pp. 202–213, 2021.
[20] S. Dindar, S. Kaewunruen, and M. An, "A hierarchical bayesian-based model for hazard analysis of climate effect on failures of railway turnout components," *Reliability Engineering & System Safety*, vol. 218, p. 108130, 2022.
[21] X. Zhang and S. Mahadevan, "Bayesian network modeling of accident investigation reports for aviation safety assessment," *Reliability Engineering & System Safety*, vol. 209, p. 107371, 2021.
[22] T. Bian, H. Zheng, L. Yin, and Y. Deng, "Failure mode and effects analysis based on d numbers and topsis," *Quality and Reliability Engineering International*, vol. 34, no. 4, pp. 501–515, 2018.
[23] X. Su, S. Mahadevan, P. Xu, and Y. Deng, "Dependence assessment in human reliability analysis using evidence theory and ahp," *Risk Analysis*, vol. 35, no. 7, pp. 1296–1316, 2015.
[24] H. Zhang and Y.-F. Li, "Integrated optimization of test case selection and sequencing for reliability testing of the mainboard of internet backbone routers," *European Journal of Operational Research*, 2021.
[25] K. Guo and L. Zhang, "Adaptive multi-objective optimization for emergency evacuation at metro stations," *Reliability Engineering & System Safety*, vol. 219, p. 108210, 2022.
[26] C. Shao and Y. Li, "Optimal defense resources allocation for power system based on bounded rationality game theory analysis," *IEEE Transactions on Power Systems*, 2021.
[27] F. Xiao, "CEQD: A complex mass function to predict interference effects," *IEEE Transactions on Cybernetics*, p. DOI: 10.1109/TCYB.2020.3040770, 2021.
[28] F. Xiao, "CaFtR: A fuzzy complex event processing method," *International Journal of Fuzzy Systems*, pp. 1–14, 2021.
[29] Y. Gao, B. Kong, and K. M. Mosalam, "Deep leaf-bootstrapping generative adversarial network for structural image data augmentation," *Computer-Aided Civil and Infrastructure Engineering*, vol. 34, no. 9, pp. 755–773, 2019.
[30] T. Zhou, W. Wu, L. Peng, M. Zhang, Z. Li, Y. Xiong, and Y. Bai, "Evaluation of urban bus service reliability on variable time horizons using a hybrid deep learning method," *Reliability Engineering & System Safety*, vol. 217, p. 108090, 2022.
[31] Y. Yao, J. Wang, P. Long, M. Xie, and J. Wang, "Small-batch-size convolutional neural network based fault diagnosis system for nuclear energy production safety with big-data environment," *International Journal of Energy Research*, vol. 44, no. 7, pp. 5841–5855, 2020.
[32] Y. Gao, P. Zhai, and K. M. Mosalam, "Balanced semisupervised generative adversarial network for damage assessment from low-data imbalanced-class regime," *Computer-Aided Civil and Infrastructure Engineering*, vol. 36, no. 9, pp. 1094–1113, 2021.
[33] J. Yin, X. Ren, R. Liu, T. Tang, and S. Su, "Quantitative analysis for resilience-based urban rail systems: A hybrid knowledge-based and data-driven approach," *Reliability Engineering & System Safety*, vol. 219, p. 108183, 2022.
[34] R. Guimera, S. Mossa, A. Turtschi, and L. N. Amaral, "The worldwide air transportation network: Anomalous centrality, community structure, and cities' global roles," *Proceedings of the National Academy of Sciences*, vol. 102, no. 22, pp. 7794–7799, 2005.
[35] Y. Zhang and S. T. Ng, "Robustness of urban railway networks against the cascading failures induced by the fluctuation of passenger flow," *Reliability Engineering & System Safety*, vol. 219, p. 108227, 2022.
[36] J. Boakye, R. Guidotti, P. Gardoni, and C. Murphy, "The role of transportation infrastructure on the impact of natural hazards on communities," *Reliability Engineering & System Safety*, vol. 219, p. 108184, 2022.
[37] E. Hernández-Perdomo, C. M. Rocco, and J. E. Ramirez-Marquez, "Node ranking for network topology-based cascade models–an ordered weighted averaging operators' approach," *Reliability Engineering & System Safety*, vol. 155, pp. 115–123, 2016.
[38] F. Liu, Z. Wang, and Y. Deng, "GMM: A generalized mechanics model for identifying the importance of nodes in complex networks," *Knowledge-Based Systems*, vol. 193, p. 105464, 2020.
[39] J. E. Ramirez-Marquez, C. M. Rocco, K. Barker, and J. Moronta, "Quantifying the resilience of community structures in networks," *Reliability Engineering & System Safety*, vol. 169, pp. 466–474, 2018.
[40] A. López-Cuevas, J. Ramírez-Márquez, G. Sanchez-Ante, and K. Barker, "A community perspective on resilience analytics: A visual analysis of community mood," *Risk Analysis*, vol. 37, no. 8, pp. 1566–1579, 2017.
[41] D. Wei, X. Zhang, and S. Mahadevan, "Measuring the vulnerability of community structure in complex networks," *Reliability Engineering & System Safety*, vol. 174, pp. 41–52, 2018.
[42] C. M. Rocco S. and J. E. Ramirez-Marquez, "Vulnerability metrics and analysis for communities in complex networks," *Reliability Engineering & System Safety*, vol. 96, no. 10, pp. 1360–1366, 2011.
[43] H. Wang, Y.-P. Fang, and E. Zio, "Risk assessment of an electrical power system considering the influence of traffic congestion on a hypothetical scenario of electrified transportation system in new york state," *IEEE Transactions on Intelligent Transportation Systems*, 2019.
[44] X. Zhang, Z. Hu, and S. Mahadevan, "Bilevel optimization model for resilient configuration of logistics service centers," *IEEE Transactions on Reliability*, 2020.
[45] Z. Enrico, S. Giovanni, M. Roberto, and M. Giovanna, "Analysis of the safety efficiency of a road network: a real case study," *Reliability:*

Theory & Applications, vol. 3, no. 2 (9), 2008.
[46] X. Zhang, S. Mahadevan, S. Sankararaman, and K. Goebel, "Resilience-based network design under uncertainty," *Reliability Engineering & System Safety*, vol. 169, pp. 364–379, 2018.
[47] P. M. Panayides, "Maritime logistics and global supply chains: towards a research agenda," *Maritime Economics & Logistics*, vol. 8, no. 1, pp. 3–18, 2006.
[48] S. Fu, D. Zhang, E. Zio, Y. Wang, and X. Yan, "Framework for quantitative resilience analysis of maritime transportation systems from risk perspectives: A case study of a ship stuck in ice in arctic waters," in *26th European Safety and Reliability Conference, ESREL 2016*, pp. 359–359, CRC Press/Balkema, 2017.
[49] A. Calatayud, J. Mangan, and R. Palacin, "Vulnerability of international freight flows to shipping network disruptions: a multiplex network perspective," *Transportation Research Part E: Logistics and Transportation Review*, vol. 108, pp. 195–208, 2017.
[50] S. Faghih-Roohi, M. Xie, and K. M. Ng, "Accident risk assessment in marine transportation via markov modelling and markov chain monte carlo simulation," *Ocean Engineering*, vol. 91, pp. 363–370, 2014.
[51] S. A. Zarghami and J. Dumrak, "Unearthing vulnerability of supply provision in logistics networks to the black swan events: Applications of entropy theory and network analysis," *Reliability Engineering & System Safety*, p. 107798, 2021.
[52] H. Dui, X. Zheng, and S. Wu, "Resilience analysis of maritime transportation systems based on importance measures," *Reliability Engineering & System Safety*, vol. 209, p. 107461, 2021.
[53] F. Goerlandt and S. Islam, "A bayesian network risk model for estimating coastal maritime transportation delays following an earthquake in british columbia," *Reliability Engineering & System Safety*, vol. 214, p. 107708, 2021.
[54] M. Kitsak, L. K. Gallos, S. Havlin, F. Liljeros, L. Muchnik, H. E. Stanley, and H. A. Makse, "Identification of influential spreaders in complex networks," *Nature Physics*, vol. 6, no. 11, pp. 888–893, 2010.
[55] S. N. Dorogovtsev, A. V. Goltsev, and J. F. F. Mendes, "K-core organization of complex networks," *Physical Review Letters*, vol. 96, no. 4, p. 040601, 2006.
[56] Z. Li, T. Ren, X. Ma, S. Liu, Y. Zhang, and T. Zhou, "Identifying influential spreaders by gravity model," *Scientific Reports*, vol. 9, no. 1, pp. 1–7, 2019.
[57] S. Li and F. Xiao, "The identification of crucial spreaders in complex networks by effective gravity model," *Information Sciences*, vol. 578, pp. 725–749, 2021.
[58] S. Brin and L. Page, "The anatomy of a large-scale hypertextual web search engine," *Computer Networks and ISDN Systems*, vol. 30, no. 1-7, pp. 107–117, 1998.
[59] G. Chen, X. Wang, and X. Li, *Introduction to complex networks: models, structures and dynamics*. Higher Education Press, 2012.
[60] A. Rényi, "On measures of entropy and information," in *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics*, pp. 547–561, University of California Press, 1961.
[61] H. Li and F. Xiao, "A method for combining conflicting evidences with improved distance function and tsallis entropy," *International Journal of Intelligent Systems*, vol. 35, no. 11, pp. 1814–1830, 2020.
[62] X. Gao, F. Liu, L. Pan, Y. Deng, and S.-B. Tsai, "Uncertainty measure based on tsallis entropy in evidence theory," *International Journal of Intelligent Systems*, vol. 34, no. 11, pp. 3105–3120, 2019.
[63] P. Bonacich, "Factoring and weighting approaches to status scores and clique identification," *Journal of mathematical sociology*, vol. 2, no. 1, pp. 113–120, 1972.
[64] R. Criado, J. Flores, B. Hernández-Bermejo, J. Pello, and M. Romance, "Effective measurement of network vulnerability under random and intentional attacks," *Journal of Mathematical Modelling and Algorithms*, vol. 4, no. 3, pp. 307–316, 2005.
[65] S. Boccaletti, J. Buldú, R. Criado, J. Flores, V. Latora, J. Pello, and M. Romance, "Multiscale vulnerability of complex networks," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 17, no. 4, p. 043110, 2007.
[66] L. C. Freeman, "A set of measures of centrality based on betweenness," *Sociometry*, pp. 35–41, 1977.
[67] V. Latora and M. Marchiori, "A measure of centrality based on network efficiency," *New Journal of Physics*, vol. 9, no. 6, p. 188, 2007.
[68] H. Liu, Z. Tian, A. Huang, and Z. Yang, "Analysis of vulnerabilities in maritime supply chains," *Reliability Engineering & System Safety*, vol. 169, pp. 475–484, 2018.
[69] S. Oldham, B. Fulcher, L. Parkes, A. Arnatkeviciute, C. Suo, and A. Fornito, "Consistency and differences between centrality measures across distinct classes of networks," *PloS One*, vol. 14, no. 7, p. e0220061, 2019.
[70] D. L. Alderson, D. Funk, and R. Gera, "Analysis of the global maritime transportation system as a layered network," *Journal of Transportation Security*, vol. 13, no. 3, pp. 291–325, 2020.
[71] N. N. Taleb, *The black swan: The impact of the highly improbable*, vol. 2. Random house, 2007.
[72] T. Wen and Y. Deng, "The vulnerability of communities in complex networks: An entropy approach," *Reliability Engineering & System Safety*, vol. 196, p. 106782, 2020.
[73] T. Wen, J. Cao, and K. H. Cheong, "Gravity-based community vulnerability evaluation model in social networks: GBCVE," *IEEE Transactions on Cybernetics*, 2021.