Analysis of Vulnerabilities in Maritime Supply Chains

Honglu Liu[∀1], Zhihong Tian[*2,4], Anqiang Huang[3], Zaili Yang[*4]
1.Beijing Jiaotong University
2.Beijing Institute of Graphic Communication
3. Beijing Jiaotong University
4. Liverpool Logistics, Offshore and Marine Research Institute,
Liverpool John Moores University

Abstract: This paper aims to analyze the different concepts of "vulnerability" used in maritime supply chains, and to develop a novel framework with supporting models to identify and analyze the relevant vulnerabilities in the chains. A real case of the Maersk shipping line in its Asia-Europe route is studied to demonstrate the applicability of the proposed framework. We find that the investigated network has stronger robustness against random failures than that when facing deliberate attacks. Furthermore, to identify vulnerable nodes (i.e. ports) of the network, two different types of analysis are undertaken through a multi-centrality model and a robustness analysis model, respectively. Consequently, the vulnerabilities estimated through robustness analysis can ascertain those by the classical centrality methods when they appear on both analysis results. More importantly, the similarity between the two outcomes can help gain more confidence on the accuracy in terms of the identification of the vulnerabilities in the system, while the difference (if any) such as those identified by the robustness analysis but not by the centrality analysis (or vice versa) can trigger a further investigation to find the comprehensive vulnerable nodes against different threats/hazards. It will aid rational decision on design and operation of resilient and robust maritime supply chains.

Keyword: vulnerability; maritime transport; complex network; network topology; network robustness, resilience, maritime risk

1 Introduction

With the fast development of container transportation, maritime supply chains become one of the largest complex networks in the world. Random failures and deliberate attacks[1] on a single element (node or edge) in the network may cause a cascading breakdown of the whole system. Foci of investigating the risks associated with the chains are moving from classical cause-consequence analysis at a local component level to a network vulnerability study from a global system perspective. Complex network theories and methods,

[∀] The first two authors contribute equally to this work as the co-first authors.

[*] Corresponding authors: tianzhihong@bigc.edu.cn; z.yang@ljmu.ac.uk.

[1] Random failures refer to the random removals of the nodes/edges in a network to see their impact to the global network efficiency, while deliberate attacks mean the selected removals of the nodes/edges based on their topological importance from high to low in a network structure.

including Social Network Analysis (SNA) and system simulation, are therefore playing increasingly important roles in the vulnerability anlysis of maritime supply chains (González *et al*. 2012; Berle *et al*. 2011; Lhomme *et al*. 2015).

A careful literature review on maritime and supply chain vulnerabilities reveals three main research challenges in previous studies. First, the maritime sector received little attention in terms of both complex networks and resilience and vulnerability research, compared to other transportation networks (Kaluza *et al.* 2010). Most of existing risk studies in maritime transport networks are from safety and security perspectives (e.g. Yang et al., 2010; 2013; 2014; 2016). Secondly, the concept of the term "vulnerability" used in this field significantly varies with regards to different research contexts, requiring the new development of a consolidated definition and a systematic research framework. Thirdly, from a theoretical perspective, vulnerability of complex networks were analyzed by using either centrality measures in SNA or robustness analysis approaches, but not in a combined way yet. Comparative analysis using both methods are scanty, requiring investigation to explore the associated potential benefits. To fill such research gaps, this paper aims to analyze the different concepts of "vulnerability" used in maritime supply chains, and to develop a novel framework with supporting models to identify and analyze the relevant vulnerabilities in maritime supply chains. The research findings from both SNA and robustness analysis approaches will be compared to provide useful insights for ship lines to identify the vulnerable nodes in their network for accident prevention.

The remaining part of this paper is organized as follows. In Section 2, the relevant literature on "vulnerability" is reviewed. In Section 3, a new methodology for the vulnerability analysis of maritime supply chains is developed while maritime network modeling, and its basic topology features are analyzed in Section 4. In Section 5, a model of two indexes, global and local network efficiency, is built to evaluate the network robustness. In Section 6, multi-centrality models based on the Borda Count method and robustness analysis approaches are developed to identify vulnerable ports in maritime networks through the evaluation of the relative drop of the network efficiency. Finally, Section 7 describes the research implications and discusses, while Section 8 concludes the paper by highlighting its contributions and limits.

2 Literature review

According to the literature study, the concepts of the term "vulnerability" vary within different research contexts. There are three main kinds of relevant definitions.

(1) First, the network vulnerability is the opposite perspective of the concept "network robustness", which denotes how the network topology (or further one, e.g., the network performance, usually including global and local connection properties) is affected by the elimination of a finite number of links and/or nodes. In other words, the "vulnerability" denotes the decrease of network performance due to a random or selected removal of nodes or edges (Holme *et al.* 2002).

Measures used to evaluate the network performance are found in different research areas, such as the degradation of the global safety efficiency of power grids (Eusgeld *et al.* 2009), the net-ability of power grids (Bompard *et al.* 2009), network connectivity of transport flows (Ducruet *et al.* 2012). It is observed that the more heterogeneous a network is, in term of, e.g., degree distribution, the more robust it is, to random failures, while, at the same time, it appears more vulnerable to deliberate attacks on highly connected nodes (Barabási *et al.* 1999, Albert *et al.* 2000). This kind of vulnerability reflects the integral property of the whole network.

In order to avoid unnecessary confusion, in our research, the term "network vulnerability" is replaced by "network robustness". After building a maritime network, the drop of global and local network efficiency[2] which is generally defined as a function of the fraction of the removed nodes, will be investigated.

(2) Secondly, vulnerability is related to the importance of elements (links or nodes). The term "importance" is intended to qualify the role that the presence and location of a specific element play with respect to the average global and local connection properties of the whole network. In this kind of context, researchers deem that the most important elements are the most vulnerable ones in the whole network, and identification of the important elements becomes their key research goals. There are two ways to identify the most important elements, a direct way and an indirect way. The direct one is to design and calculate the direct measurements to identify the most important elements. For example, there are various kinds of centralities in the relevant literature (Sabidussi 1966, Xu *et al.* 2007, Hu *et al.* 2009, Laxe*et al.* 2012, Ducruet *et al.* 2012). In addition, the indirect way is to measure the drop of network performance when given elements are removed (Latora *et al.* 2005, Zio *et al.* 2008). In this research, both methods are investigated in order to get a comprehensive solution.

(3) Thirdly, some researchers define the term "node vulnerability" by the node dependence which is a local property. In a weighted maritime network, node dependence can be defined as the share of the dominant flow connection within total transport traffic which is an inversely proportionate relation between the number of connections and the distribution of traffic among those connections (Ducruet *et al.* 2010, Laxe *et al.* 2012). Hence, nodes (i.e. ports) with lower vulnerability are those which are less dependent with respect to others located in their foreland.

In this research, the first two concepts are investigated in a combined manner in the maritime transport context, one is "network robustness" analyzed in Section 5, and the other one is "important node" related to the whole network vulnerability, which is investigated in Section 6. By investigating the similarity between them, the vulnerability in maritime supply chains is defined as "the measure of the impact of the nodes and links to the network robustness" in this paper.

3 Methodology

According to the above definition of vulnerability, the methodology proposed in this work is developed based on the measurement instruments in the complex network theory. The first step is to use data sources to build the maritime supply network under investigation. Next, the measures using centrality and robustness analysis are carried out to analyze vulnerability in the network. Last, when more information about the network is acquired, an in-depth (focused) analysis will be conducted. The framework, visually presented in Figure 1 is explained in Section 3.1, providing a foundation for more research on the vulnerability analysis of maritime transport networks in future.

3.1 Research framework

Eusgeld *et al.* (2009) proposed a framework for the vulnerability analysis of critical infrastructures, which based on a problem-driven iterative approach, includes five main steps, several decision points and

[2] The detailed definitions and algorithms relating to the drop of network efficiency are provided in Section 5.

feedback loops. By simplifying the framework and also incorporating the complex network theory and the characteristics of maritime transport networks, we propose a four-step framework for maritime vulnerability analysis in this paper.

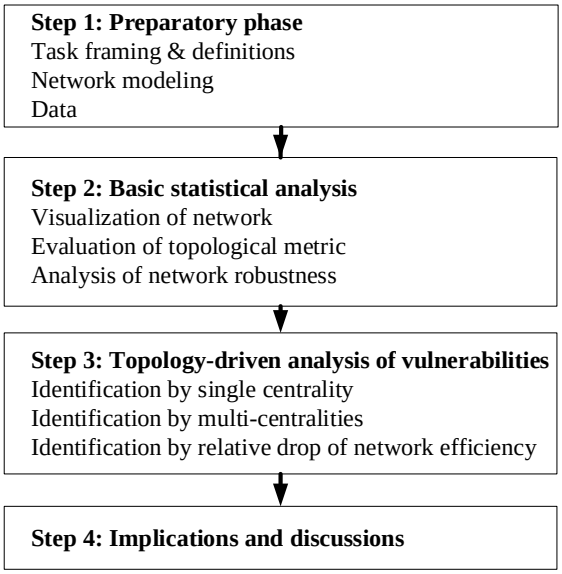

Figure 1. Research framework for vulnerability analysis of maritime supply chains

In Figure 1, the preparatory phase aims at reaching a clear definition of the terms and mutual understanding of the objectives between all parties which have a stake in the analysis of the network and its operation. The next step ‘‘Basic statistical analysis’’ focuses on the development of systematic understanding for the robustness analysis of the network. Step 3 is to identify important nodes/links by topology-driven analysis of vulnerabilities. Step 4 is to describe the implications from and discussions on the findings by incorporating the other information about the network and the associated environments in which it operates for meaningful conclusions.

3.2 Maritime network modeling

The typical definition of a maritime transport network is a graph where nodes are ports and links are inter-port connections realized by the circulation of vessels. In other words, the network is built based on vessel characteristics, ports of call and vessel movements. The links could be directed or non-directed links, weighted or non-weighted links, depending on the demand of research.

In 2007, Xu *et al.* (2007) introduced the idea of space *L* and *P* into maritime networks, and extended the idea to the case of directed networks. The first topological representation is the space *L*, which consists of nodes being ports, and a link between two nodes which exists if they are consecutive stops on a ship route. The node degree *k* in this topology is just the number of different ship lines one can take from a given port. The distance in such a space is measured by the total number of stops passed on the shortest path between two nodes. The second representation is the space *P*, in which an edge is formed between two nodes when they are in the same route that a container ship passes through. Consequently, the node degree *k* in this topology represents the total number of nodes reachable using a single ship route and the distance can be interpreted as the number of transfers (plus one) one has to take from one port to another.

Hu *et al.* (2009) also used the above two different network representations to construct the worldwide maritime transportation network. Ducruet *et al.* (2010) provided two concepts of GDL (Graph of Direct Links) and GAL (Graph of All Links) to replace the spaces *L* and *P* (Ducruet & Zaidi 2012; Ducruet & Notteboom 2012). The GDL only includes direct successive calls between ports (namely from port A to port B and from port B to port C), while the GAL includes direct and indirect calls. It can be argued that two ports can also be connected if they belong to the same liner service or loop, although they are not adjacent calls (that is from port A to port C). Therefore, in this research, the network type space *L* (GDL) (Seaton *et al.* 2004, Xu *et al.* 2007, Ducruet *et al.* 2010) is considered, which consists of nodes (*i.e.*, ports), and a link between two nodes exists if they are consecutive stops on the same ship route.

3.3 Data source and visualization

The data source in our research is from the Maersk shipping line with a focus on its Asia-Europe routes in July 2014 from Maersk website (http://www.maerskline.com), including 19 shipping lines and 54 calling ports. Table 1 shows the index number of each port.

Table 1. Port index and its name

Index	**Port name**	**Index**	**Port name**
1	Aarhus	28	Le havre
2	Algeciras	29	Marsaxlokk
3	Ambarli	30	Nagoya
4	Antwerp	31	Nansha
5	Barcelona	32	Nansha new port
6	Beirut	33	Ningbo
7	Bremerhaven	34	Odessa
8	Busan	35	Port Klang
9	Chiwan	36	Port Said
10	Colombo	37	Port tangiers
11	Constantza	38	Qingdao
12	Dalian	39	Rijeka
13	Felixstowe	40	Rotterdam
14	Fossurmer	41	Salalah
15	Gdansk	42	Shanghai
16	Genoa	43	Singapore
17	Gothenburg	44	Suez canal container terminal (SCCT)
18	Hamburg	45	Tanjungpelepas
19	Hong Kong	46	Trieste
20	Ilyichevsk	47	Valencia
21	Izmitkorfezi	48	Vungtao
22	Jebel all	49	Wilhelmshaven
23	Jeddah	50	Xiamen
24	Kobe	51	Xingang
25	Koper	52	Yantian

26	Kwangyang	53	Yokohama
27	La spezia	54	Zeebrugge

An adjacency matrix $\boldsymbol{A}$ represents the links connecting each pair of nodes. The element a_{ij} of the adjacent matrix $\boldsymbol{A}$ equals to 1 if there is a link from node i to j or 0 if there is not a link. If a network is directed, meaning that edges point in one direction from one node to another node, then a node has two different degrees, the in-degree $k_{in}(i)$, which counts the number of its incoming edges, and the out-degree k_{out} (i), which is the total number of its outgoing edges (Xu *et al.* 2007, Hu *et al.* 2009).

$$k_{in}(i) = \sum_{j\neq i} a_{ji}\,, k_{out}(i) = \sum_{j\neq i} a_{ij}, k_{all}\,(i) = \sum_{j\neq i}(a_{ji} \text{or} a_{ij}) \quad (1)$$

Because shipping routes are directed, links in the network should also be directed. From the asymmetric adjacent matrix $\boldsymbol{A}$, three kinds of degrees (i.e. in-degree, out-degree and all-degree) can be calculated.

In addition, traffic on a transportation network is usually not equally distributed. Some links have more traffic flows than others, hence playing more important roles in the functioning of the whole network. Weighting should be addressed accordingly. In this study, we assume* that the more shipping lines from port i to port j are, the greater the weight of the link from i to j. The element w_{ij} of the link weight matrix $\boldsymbol{W}$ is usually used to represent the strength or importance of relations from port i to port j (Xu *et al.* 2007; Hu *et al.* 2009). We define the element w_{ij} of the weight matrix $\boldsymbol{W}$ is the number of shipping lines passing from port i to port j (Hu *et al.* 2009). Then, another important metric is deduced, called node strength. Node strength is defined as the total weight of adjacent connections of a node. The strength distribution is a characteristic of a node. It is also divided into in-strength $s_{in}(i)$, out-strength $s_{out}(i)$, and all-strength $s_{all}(i)$, in our network.

$$s_{in}(i) = \sum_{j\neq i} w_{ji}\,, s_{out}(i) = \sum_{j\neq i} w_{ij}\,, s_{all}(i) = \sum_{j\neq i}(w_{ij} + w_{ji}) \quad (2)$$

Finally, the investigated network contains 54 nodes and 132 directed and weighted edges. The network visualization is shown in Figure 2. The size of the edges reflects the weights of the associated links.

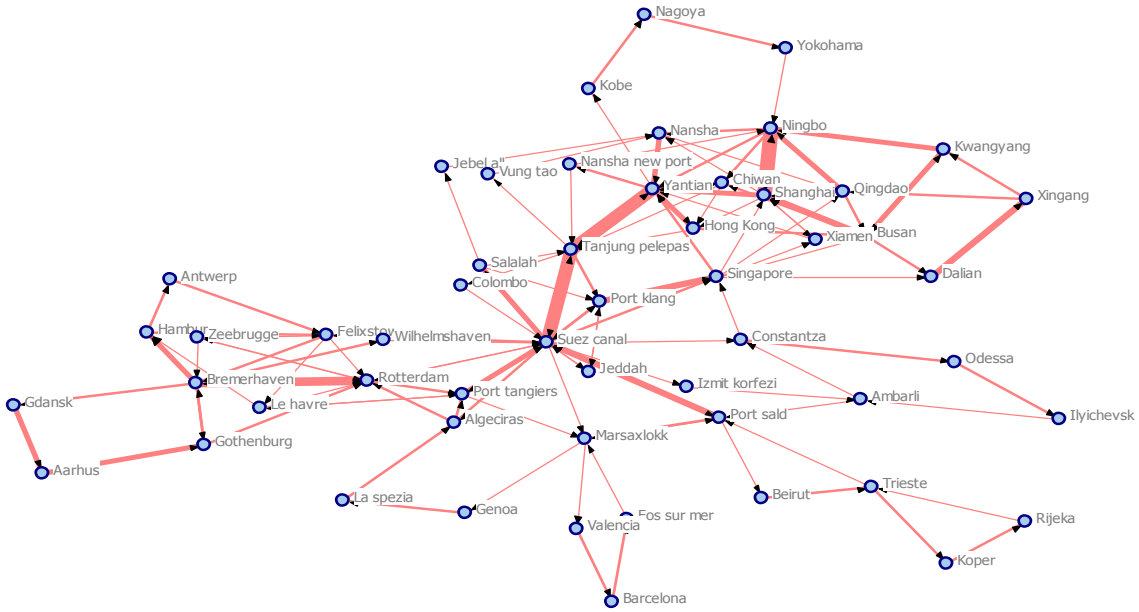

Figure 2.Visualization of network

* The specific data on cargo throughput in ports and routes is not publically available with respect to the Maersk line. However, it can be easily incorporated into the weighting analysis when it becomes available, hence having no significant effect on the demonstration of the feasibility of the proposed framework in the paper.

4. Analysis on network topology features

4.1 Degree metrics and their distributions

The above Figure 2 only shows the network topology. It is necessary to use statistical methods to further investigate the feature of the network topology. In statistics, the topology structure of a network can be analyzed by distribution functions. The spread in the number of edges of a node, *i.e.*, node degree, is characterized by a distribution function $P(k)$, which describes the probability that a random selected node i has exactly k_i edges. Emergence of a power-law in the degree distribution $P(k) \sim k^{-\gamma}$ in complex networks is an interesting self-organized phenomenon in complex systems. Such a network is called scale-free network. In this section, the degree distributions of the 54 nodes in Table 1 are analyzed using Eq. (1). The out-degree, in-degree and all-degree of each port are calculated and presented in Figure 3.

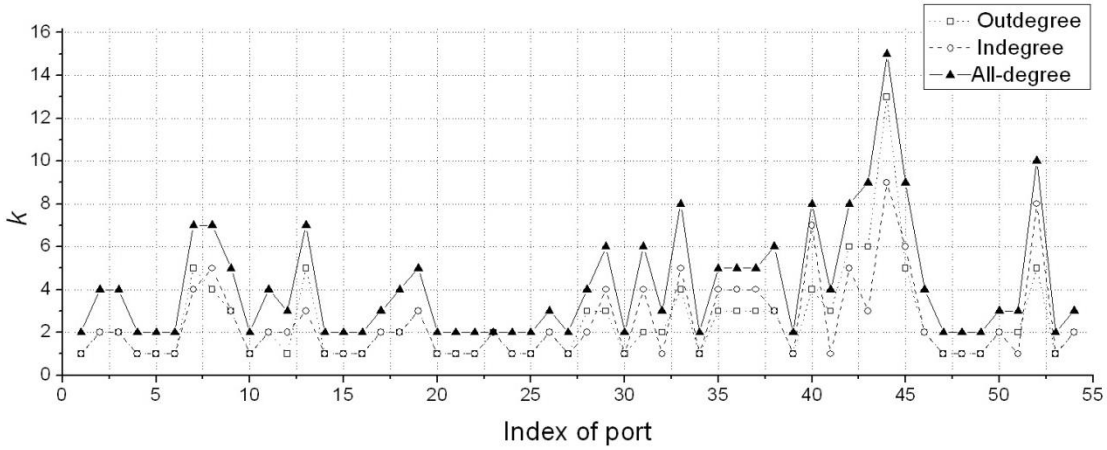

Figure 3. Out-degree, in-degree and all-degree according to each port

The cumulative degree distribution function $P(k)$ of in-degree and out-degree (Newman, 2003) are calculated and presented in Figure 4, respectively. In order to investigate the topology structure feature of the network, the power-law fitting is carried out in a log-log coordinate.

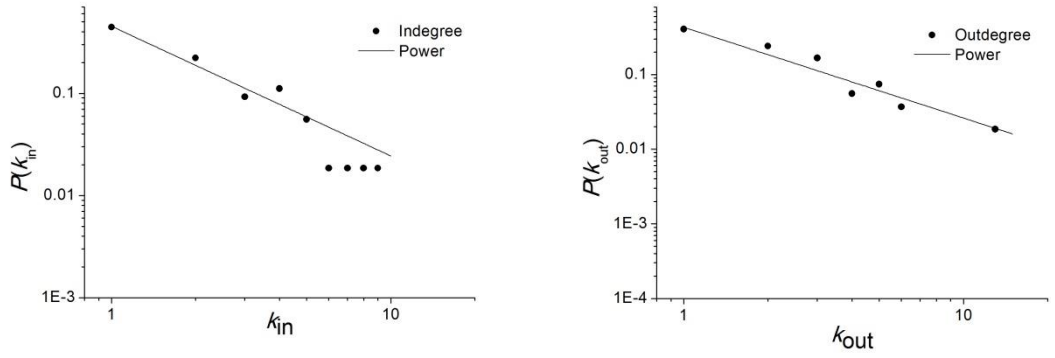

Figure 4. In-degree and out-degree distributions in a log-log coordinate

In Figure 4, the left subfigure presents the power-law fitting curve of the in-degree distribution, which is $p(k_{in})=0.453a*k_{in}^{-1.269b}$, a=0.453, b=-1.269, with R-square as 0.9739, and adjusted R-square as 0.9702 in a normal coordinate. The right subfigure describes the power-law fitting curve of the out-degree distribution in a normal coordinate. The power-law fitting curve is $p(k_{out})= 0.4293*k_{out}^{-1.216b}$, a=0.4293, b=-1.216, with R-square as 0.9312 and adjusted R-square as 0.925. Similarly, the power-law fitting curve of the all-degree distribution is obtained and shown in Figure 5, in which the power-law fitting curve of all-degree distribution is $p(k)= 1.404*k^{-1.838}$ with R-square as 0.9586 and adjusted R-square as 0.9552.

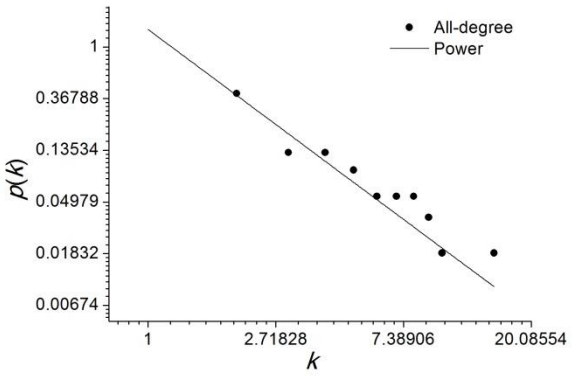

Figure 5. Degree distribution of a non-directed network in a log-log coordinate

Consequently, the power-law fitting curves of the in-degree, out-degree and all-degree distributions, tending to follow a power law-like distribution, imply the existence of several hub ports in the investigated network, which occupy a majority of shipping routes.

4.2 Node strength metrics and their distributions

The in-strength, out-strength and all-strength values of each port are calculated using Eq. (2) and shown in Figure 6.

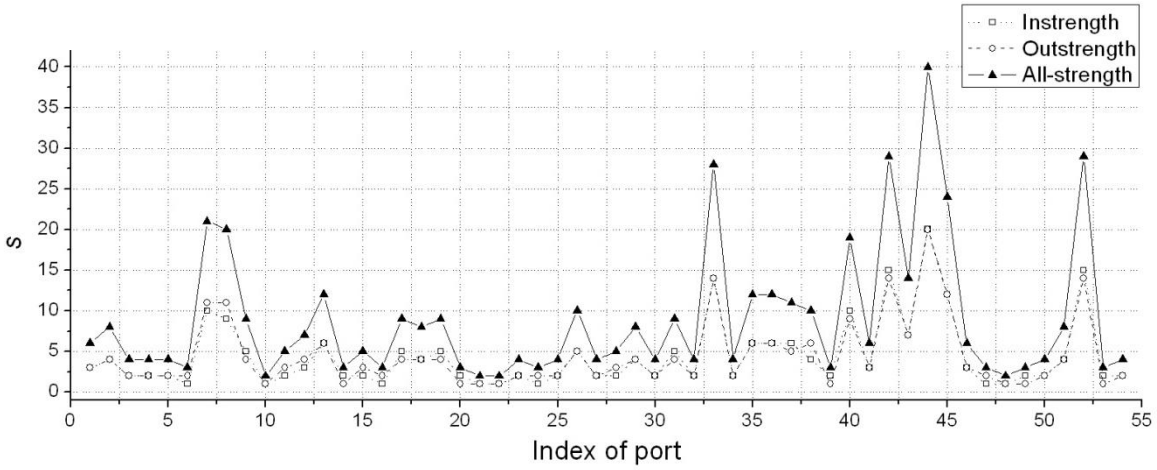

Figure 6. In-strength, out-strength and all-strength values of each port

The cumulative node strength distribution functions $P(s)$ of in-strength and out-strength are presented in

Figure 7. In order to investigate the structure feature of the network, the power-law fitting is carried out in a log-log coordinate.

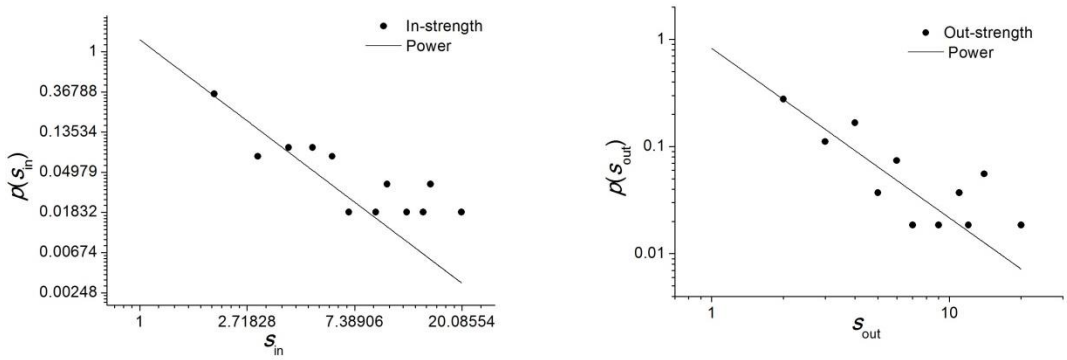

Figure 7. In-strength and out-strength distributions in a log-log coordinate.

In Figure 7, the left subfigure presents the power-law fitting curve of the in-strength distribution is $p(s_{in})= 1.35*s_{in}^{-2.021}$ with R-square as 0.9021 and adjusted R-square as 0.8963. The right subfigure describes the power-law fitting curve of the out-strength distribution is $p(s_{out})= 0.8259*s_{out}^{-1.583}$ with R-square as 0.8613 and adjusted R-square as 0.8531. Similarly, the power-law fitting curve of the all-strength distribution is obtained and shown in Figure 8. The part of the distribution exhibits a power law-like degree distribution.

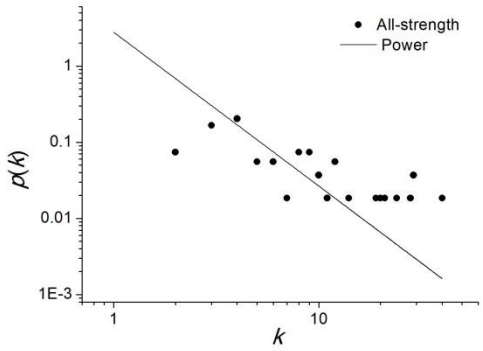

Figure 8. Strength distribution of non-directed network in a log-log coordinate.

In Figure 8, the power-law fitting curve of the all-degree distribution is $p(k)= 2.79*k^{-2.02}$ with R-square as 0.7511 and adjusted R-square as 0.744.

It is clear that any of the in-strength, the out-strength and all-strength distributions follows a power law-like distribution. Such a result implies that several hub ports connect with the majority of the shipping lines in the network, and the rest ports associate with very few lines. Therefore, from the node strength perspective, the investigated network can be regarded as scale-free and heterogeneous.

If random attacks occur on a heterogeneous network of ports, it is less likely to happen on the hub ports and will therefore not have a huge impact on the structure and function of the whole system. However, once failures occur on any of the hub ports, the impact would spread quickly throughout the whole network.

5 Network robustness

Network robustness denotes the capacity to resist the effect of a random or selected removal of nodes or edges. From the definition, it can be seen that network robustness could be analyzed from two perspectives of random failures of and deliberate attacks to ports.

From the above node degree and strength analysis, the investigated network is obviously heterogeneous. In general, a heterogeneous network has stronger robustness against random failures but weaker robustness against deliberate attacks, given that deliberate attacks target more on highly connected nodes (Barabási *et al.* 1999, Albert *et al.* 2000). To measure the network performance with more precision, some metrics are proposed based on the network connectivity, such as average shortest path length (Albert *et al.* 2000), network efficiency (Latora *et al.*2001), and largest cluster size (Barabási *et al.* 1999, Albert *et al.* 2000). Hence, in this section, we investigate the network robustness by two measures of network performance which are global network efficiency *E* and local efficiency clustering coefficient *C* (Latora *et al.* 2001).

5.1 Global network efficiency

Latora *et al.* (2001) have introduced the concept of efficiency of a network, which measures how efficiently the information is exchanged over the network. In general, the efficiency of a network relates to the shortest distance of each pair of nodes, because information spreads rapidly along a network with a small shortest path length (Latora *et al.* 2003, Wang *et al.* 2006).

The efficiency ε_i in the communication between node *i* and *j* is inversely proportional to the shortest path: $\varepsilon_i = \frac{1}{l_{ij}}, \forall i,j$. The efficiency *E* of a network with *n* nodes can be defined as (Latora *et al.* 2001, Ducruet *et al.* 2012):

$$E(G) = \frac{\sum_{i \neq j \in G} \varepsilon_i}{n(n-1)} = \frac{\sum_{i \neq j \in G} \frac{1}{l_{ij}}}{n(n-1)} \quad (3)$$

where l_{ij} is the shortest path length between node *i* and *j*. The maximum value *E* reaches to 1 when the network is fully connected, and the minimum value decreases to 0 when all nodes are isolated ($E \in [0,1]$).

In our analytical process, nodes are separated from the network by two strategies which are the random failures (i.e. random removal) and deliberate attacks (i.e. selected removal). Using the random failure strategy, the nodes are removed randomly, while under the deliberate attack strategy the nodes are removed in order from the highest to the lowest degrees. The corresponding dynamics of the network efficiency *E* against the aggregated ration of the removal nodes *f* are calculated using Eq. (3) and shown in Figure 9.

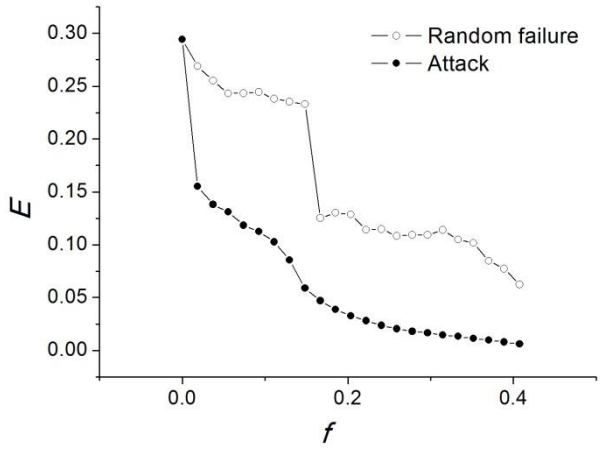

Figure 9. Dynamics of the network efficiency *E* against the ratio *f* of the removed nodes.

Figure 9 shows that, as nodes are separated from the network, deliberate attacks result in a remarkable drop, and the network efficiency descends to 0 quickly (when about 50% nodes are separated). By contrast, random failures cause a relatively small drop. The efficiency *E* has a sharp drop when *f* reaches 0.15, which indicates that a key node of high influence (i.e. connectivity) on the network efficiency is removed by the random selection strategy. This phenomenon suggests that the maritime transport network of interest in this paper is more vulnerable to deliberate attacks than random failures with regard to the network efficiency.

5.2 Local efficiency

Clustering coefficient is used to act as a proxy of local efficiency hereby. The clustering coefficient is an important concept which reflects transitivity at a local level in a complex network. Watts and Strogatz (1998) proposed so-called clustering coefficient C_i to measure local cohesiveness of the network in the neighborhood of the node i. The neighbors of a node refer to all nodes linking to the node directly. First of all, a quantity C_i, the local clustering coefficient of node i, is defined as:

$$C_i = \frac{\text{Number of edges in } G_i}{\text{maximum possible number of edges in } G_i} = \frac{\text{Nubmer of edges in } G_i}{k_i(k_i-1)/2}$$

where G_i and k_i are the sub-graph of neighbors and the number of neighbors of node i, respectively. The clustering coefficient $C(G)$ of graph G is defined as the average of C_i over all nodes.

$$C(G) = \frac{1}{n}\sum_{i\in G} C_i \tag{4}$$

The dynamics of the clustering coefficient *C* of the investigated network are calculated using Eq. (4) and presented in Figure 10.

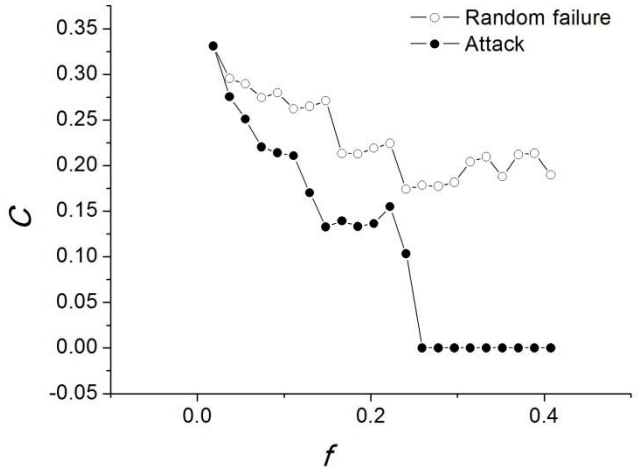

Figure 10. Dynamics of the clustering coefficient *C* against the ratio *f* of the removed nodes.

From the above Figure 10, when ports are separated from the network, deliberate attacks result in remarkable drops, and the network clustering coefficient descends to 0 quickly (when about 25% nodes are separated); in contrast, random failures cause relatively small drops, which indicates that the maritime transport is more robust when facing random failures compared to deliberate attacks with regard to the clustering coefficient.

6 Identification of important ports

Identification of important nodes presents the most practical purpose of this research for the analysis of maritime network vulnerability. It is carried out by both a multi-centrality model and a robustness analysis model. By incorporating a robustness analysis model into the identification of important nodes can complement the results by using a classical multi-centrality model only. Therefore, in practice it can provide more insights for a rational decision making.

6.1 Identification by centrality

Degree centrality

First, we identify vulnerable ports according to node degrees. From Table 2 we can see that, except port NO.44, other high-degree ports have no significant differences from each other. However, port NO.44 is Suez Canal container terminal (SCCT), which presents the gate between Europe and Asia, and obviously the analysis result verifies its importance. Other high degree ports are NO.42 (Shanghai with a high out-degree), NO.43 (Singapore with a high out-degree), NO.52 (Yantian with a high in-degree), NO.45 (Tanjungpelepas with both high in-degree and out-degree), and NO.40 (Rotterdam with a high in-degree) with specific sequences according to different degrees.

Secondly, we investigate the strength of the ports. The top 5 ports are NO.44 (SCCT), NO.42 (Shanghai), NO.52 (Yantian), NO.33 (Ningbo), NO.45 (Tanjungpelepas). Ningbo replaces Singapore, which means that more shipping lines connect with Ningbo.

Table 2. Top 5 high degree ports

Sorted by out-degree		Sorted by in-degree		Sorted by all-degree	
Port index(Name)	**Out-degree**	**Port index(Name)**	**In-degree**	**Port index(Name)**	**All-degree**
44(SCCT))	13	44(SCCT)	9	44(SCCT)	15
42(Shanghai)	6	52(Yantian)	8	52(Yantian)	10
43(Singapore)	6	40(Rotterdam)	7	43(Singapore)	9
52(Yantian)	5	45(Tanjung pelepas)	6	45(Tanjung pelepas)	9
45(Tanjung pelepas)	5	42(Shanghai)	5	42(Shanghai)	8

Betweenness centrality

We conduct the analysis on node betweenness. From Table 3 it can be seen that port NO.36 (Port Said) is an unexpected key node in the network, and other key nodes are kept in similar places to those obtained by the above methods.

Table 3. Top 4 ports based on betweenness centrality

Index(Name)	Node betweenness
44(SCCT)	1860.15
45(Tanjung pelepas)	913.667
36(Port Said)	679
52(Yantian)	628.85

Closeness centrality

The findings from closeness analysis are presented in Figure 11. Top 4 ports are listed in Table 4. NO.13 (Felixstowe), NO.35 (Port Klang) are identified due to their high out-closeness.

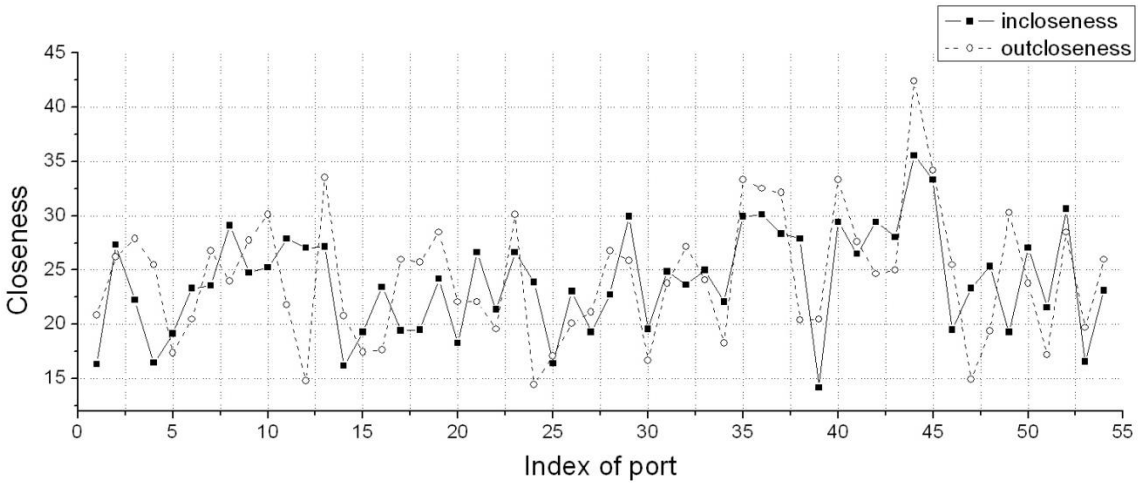

Figure 11. Closeness analysis

Table 4. Top 4 ports in terms of closeness

Sorted by incloseness		Sorted by outcloseness	
Port index(Name)	**Incloseness**	**Port index(Name)**	**Outcloseness**

44(SCCT)	35.57	44(SCCT)	42.4
45(Tanjung pelepas)	33.333	45(Tanjung pelepas)	34.194
52(Yantian)	30.636	13(Felixstowe)	33.544
36(Said)	30.114	35(Klang)	33.333

6.2 Multi-centrality model based on the Borda Count Method

In the past studies, single centrality is often used to mark the importance of ports (Xu *et al.* 2007; Hu *et al.* 2009; Laxe *et al.* 2012; Ducruet *et al.* 2012). However, single centrality provides partial information about nodes and cannot reflect the whole profile. In order to aggregate the information from different centrality measures and rank the nodes with respect to their overall role in the network, parametric approaches such as analytical hierarchy process (Bian et al., 2017), technique for order performance by similarity to ideal solution (Hu et al., 2016), fuzzy logic (Parand et al., 2016), and non-parametric ones like ordered weighted averaging (Hernández *et al.* 2016, Rocco *et al.* 2016) are used to assign a different weight to each measure. However, these methods requires to subjectively evaluate the relative importance of the selected attributes. It sometimes makes decision makers to assign more importance to some attributes over the others, which often causes subjective bias. More importantly, it constrains the presentation of each combined measure to be uniformed. To avoid the subjective bias caused by decision maker preferences, a non-parametric method based on partial order set (Rocco *et al.*, 2014) was introduced to aggregate different topological measures to rank the nodes in a network. Furthermore, voting aggregation methods like the Borda Count method (Zwicker, 1991,) and Copeland's Score method (Baroud *et al.* 2014), cutting down individual influence on the final result by electing a candidate with the broadest acceptance from all the voters, are often considered as a consensus-based approach rather than a majoritarian one. The principles of two methods are similar, while the calculation process of the Borda Count is simpler than that of Copeland's Score. The Borda Count method is used in this paper, and it is a voting method in which voters rank candidates in order of preference. Each candidate is given a certain number of points corresponding to the position in which the candidate is ranked by each voter. The candidate with the most points is the winner. It presents a rational solution in combining different measures from multi-centrality analysis as evidenced from its applications and the associated implications in recent studies (e.g. Alipour et al., 2014). In our case, all ports are the candidates, and the above centrality measures are the voters. The Borda Count method is a voting method in which voters rank candidates in order of preference. Each candidate is given a certain number of points corresponding to the position in which the candidate is ranked by each voter. The candidate with the most points is the winner. In our case, all ports are the candidates, and the above centrality measures are the voters.

In this paper, a model containing degree centrality, node strength centrality, betweenness centrality and closeness centrality is developed based on the Borda Count method. For example, there are 54 ports totally in this case, the all-degree of node No.44 ranks the first, so it gets 54 points, and the strength of this node also ranks the first, and it gets 54 points again. The total score of No.44 is 270. All ports are calculated and ranked and the result is shown in Table 5.

Table 5. Ranking of all indexed ports in terms of their aggregated centrality measures

Ranking	Index	Name	Ranking	Index	Name	Ranking	Index	Name
1	44	SCCT	19	46	Trieste	37	48	Vung tao
2	45	Tanjung pelepas	20	41	Salalah	38	34	Odessa
3	52	Yantian	21	11	Constantza	39	27	La spezia
4	40	Rotterdam	22	2	Algeciras	40	30	Nagoya
5	36	Said	23	17	Gothenburg	41	10	Colombo
6	42	Shanghai	24	50	Xiamen	42	20	Ilyichevsk
7	43	Singapore	25	3	Ambarli	43	21	Izmit korfezi
8	37	Tangiers	26	28	Le havre	44	39	Rijeka
9	33	Ningbo	27	18	Hamburg	45	6	Beirut
10	13	Felixstowe	28	54	Zeebrugge	46	24	Kobe
11	35	Port Klang	29	23	Jeddah	47	14	Fos sur mer
12	29	Marsaxlokk	30	26	Kwangyang	48	16	Genoa
13	8	Busan	31	51	Xingang	49	5	Barcelona
14	7	Bremerhaven	32	32	Nansha new port	50	25	Koper
15	38	Qingdao	33	12	Dalian	51	15	Gdansk
16	31	Nansha	34	49	Wilhelmshaven	52	4	Antwerp
17	9	Chiwan	35	53	Yokohama	53	22	Jebel all
18	19	Hong Kong	36	47	Valencia	54	1	Aarhus

6.3 Robustness analysis model based on relative drop of network efficiency

Compared with the multi-centrality model in Section 6.2, the robustness analysis model based on relative drops of network efficiency aids to identify important nodes of network from a different perspective. The main idea of the model is to identify key ports by comparing the size of efficiency drops resulted from removing each of them from the network. The robustness analysis model proceeds as follows.

- First, compute the aggregate efficiency; denoted by E of the full network with n nodes by using Eq (3). In this study, n = 54.
- Secondly, remove the *jth* ($j = 1, \dots, n$) node from the network and figure out the remaining efficiency, denoted by E_j, of the new network with the remained $n - 1$ nodes.
- Thirdly, calculate the margin of E_j $(j = 1, \dots, n)$ against E, denoted by VE_j, using the equation of $VE_j = E - E_j$.
- Finally, sort the set of VE_j $(j = 1, \dots, n)$ in an ascending order. The higher the rank of VE_j, the more important the *jth* node.

By employing the above process, a set of network efficiency margins denoted by $\{VE_j, j = 1, \dots, 54\}$ are calculated and shown in Figure 12.

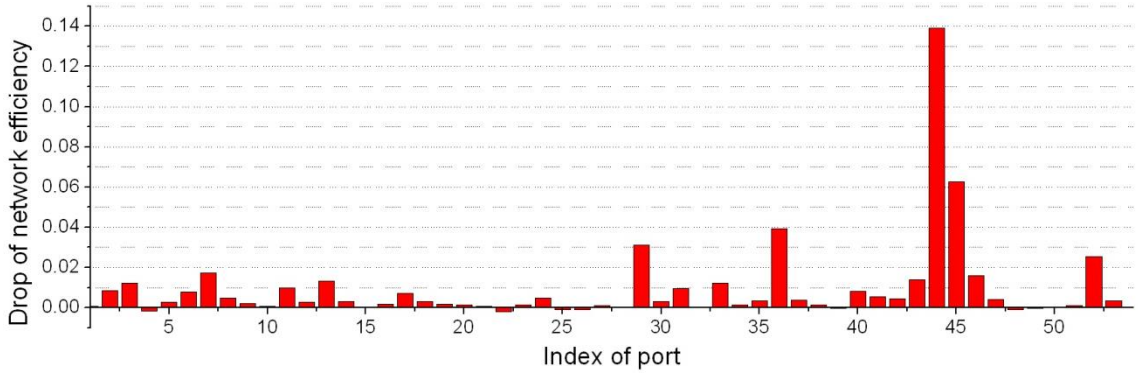

Figure 12. Network efficiency margins of separated nodes

The top 10 ports of the highest drops are listed in Table 6. In accordance with the results, the above two models (i.e. multiple centrality and robustness analysis) generate two sets of important ports of a large similarity, which casts more confidence on the findings. The inconsistency due to the different mechanisms (as well as perspectives) of the two methods suggests that the combination of two models (i.e. Tables 5 and 6) can provide more insights for rational decision on robustness and resilience of maritime supply chains. It helps avoid ignorance of any hidden important ports if and when only the traditional centrality based method is employed in vulnerability analysis of complex networks. The supportive evidence and details on the insights for rational decision are given in Section 7.

Table 6. Top 10 high drop ports

Index	**Name**
44	SCCT
45	Tanjung pelepas
36	Port Said
29	Marsaxlokk
52	Yantian
7	Bremerhaven
46	Trieste
43	Singapore
13	Felixstowe
3	Ambarli

7 Research Implications and Discussions

It should be well noted that by using the two models, *i.e.*, multi-centrality model and robustness analysis model, this study can provide more insightful analysis, including:

(1) Cross reference. The above two different approaches focus on different perspectives of node importance. The multi-centrality model focuses on the position of node and relations with other nodes from a local

node/component level. Unlike that, the method based on relative drop of network efficiency focuses on the impact of a given node on overall network connectivity from a global network perspective. The results of these two models can be cross-referenced with each other, and thus make the conclusion more reliable and convincible. For example, in accordance with the results, two sets of important ports identified by the two models have a large similarity. Six ports are commonly presented in the two lists (i.e. tables 5 and 6); furthermore, their ordering is at large consistent. Both SCCT and Tanjung pelepas are ranked 1st and 2nd; Yantian is ranked 3rd and 5th, Port Said 5th and 3rd, Singapore 7th and 8th and Felixstowe 10th and 9th, when using the centrality and robustness analysis methods respectively.

(2) Contrast analysis. By comparing the differences of the results generated by the two models, drawbacks of each individual model could be overcome and more valuable findings could be obtained. As far as the different port ranking orders are concerned, Marsaxlokk is ranked 4th by the robustness model while 12th by the multi-centrality model. From the topological structure in Figure 1, we can see that the port Marsaxlokk is the only link to port Valencia, Fossurmer and Barcelona, so deleting Marsaxlokk will lead to the separation of the three ports from other ports. Port Bremerhaven is similar to Marsaxlokk. Therefore, their importance and impact from a network perspective are evaluated higher, indicating that their roles in the vulnerability analysis of maritime supply chains are underestimated, if only classical centrality measures are used. Obviously, the hybrid of the two models generates more insightful findings. It means Port Marsxlokk and Port Bremerhaven should also be considered as vulnerable nodes for accident prevention.

(3) Managerial implications for stakeholders. The proposed analysis framework could contribute to generating valuable managerial implications for the stakeholders such as shipping lines, ports, and port states to ensure the robustness of the investigated maritime supply chains. For example, the results of our empirical study based on the data of the Maersk Line is helpful to identify key ports with respect to the vulnerability of its EU-Asia maritime network. The empirical can easily be expanded to other shipping lines.

(4) It should also be noted that this research is carried out based on route data, but the actual strategic decision making can be made by including more detailed data, *e.g.*, cargo throughput. This is one of the future research directions.

(5) Another possible research direction is to assign weights to the outcomes from the two methods for a final synthesized ranking order. The Borda Count method can be applied again by incorporating a coefficient e (e = [0, 1]). For instance, when e equals to 0.5, both methods have the same influence to the final ranking. When e equals to 0, the final ranking refers to the result from the multi-centrality method, indicating the vulnerability focuses more on the node level. When e equals to 1, the final ranking is decided by the result from the robustness analysis method, revealing that the vulnerability is conducted purely from a global network perspective.

8. Conclusion

There are scanty studies on vulnerability analysis of maritime supply chains from a complex network perspective in the current literature. Our work is a study of multi-disciplinary nature incorporating science relating to complex network, vulnerability analysis and maritime transportation operations. The findings reveal that the proposed methodology is capable of providing insights on the identification of vulnerability in maritime supply chains.

Based on related works, different concepts of vulnerability within the context of maritime networks are discussed and analyzed and a four-step research framework for study of maritime network vulnerability is

presented. Then, a real case of the Maersk shipping line on its Asia-Europe routes is studied to demonstrate the feasibility of the framework.

Main contributions of this paper can be concluded as follows. First, from the data source, basic network topology features are analyzed. All degree and strength distributions exhibit a power law-like distribution. As a result, it is found that the Asia-Europe routes of the Maersk shipping line is not homogeneous, indicating that a few hub ports occupy major shipping lines.

Secondly, network robustness is tested and analyzed in different contexts in terms of random failures and deliberate attacks. As ports are separated from the network, deliberate attacks result in remarkable drops, and the network efficiency and clustering coefficient descend to 0 quickly. In contrast, random failures cause relatively smaller drops. The network having stronger robustness against random failures, appears to be more vulnerable to deliberate attacks on highly connected nodes.

Thirdly, given that use of single centrality is arguable to provide sufficient information about vulnerability analysis of nodes for rational decision making, two methods are simultaneously conducted to identify vulnerable ports of maritime supply chains. One is the direct way through a multi-centrality model hybridizing degree centrality, node strength centrality, betweenness centrality and closeness centrality based on the Borda Count Method, while the other is the indirect way via a robustness analysis model. The results from the two models show that vulnerable nodes identified by different ways are consistent to a large extent. However the inconsistency of port ranking in terms of their vulnerability also triggers the concern that using a single method could render the ignorance of vulnerable ports when seeking solutions to ensure the resilience of maritime supply chains. The combination of two models will therefore be able to provide a more comprehensive evaluation result for aiding rational decisions.

In future research, the traffic volume of cargo throughput should be taken into account properly. In addition, the prerequisite for the research of this kind is a stable topology of the network in a fixed time window, and the dimensions of time can be investigated to reveal their impacts to the vulnerability of maritime supply chains in a dynamic manner in future work.

Acknowledgement

This research has been supported by grants from the National Natural Science Foundation of China under Grants 71540018, EU FP7 Marie Curie IRSES ENRICH project (PIRSES-GA-2013-(612546)) and the Fundamental Research Funds for the Central Universities (Grant No. B15JB00040). The authors would also like to thank the four anonymous reviewers for their constructive suggestions.

References

Albert, R., Jeong, H., & Barabási, A. L. (2010). Internet: Diameter of the world-wide web. Nature, 401(6749), 130-131.

Albert, R., Jeong, H., & Barabási, A. L. (2000). Error and attack tolerance of complex networks. Nature, 406(6794), 378-382.

Alipour, Z., Monfared, M. A. S., & Zio, E. (2014). Comparing topological and reliability-based vulnerability analysis of Iran power transmission network. Proceedings of the Institution of Mechanical

Engineers, Part O: Journal of Risk and Reliability, 228(2), 139-151.
Angeloudis, P., Bichou, K., Bell, M. G., & Fisk, D. (2007). Security and reliability of the liner container-shipping network: analysis of robustness using a complex network framework. In Risk Management in Port Operations, Logistics and Supply Chain Security, edited by K. Bichou, M. G. H. Bell, and A. Evans, 95–106. London: Informa.
Barabási, A. L., & Albert, R. (1999). Emergence of scaling in random networks. Science, 286(5439), 509-512.
Barabási, A. L. (2009). Scale-free networks: a decade and beyond. Science, 325(5939), 412.
Baroud, H., Ramirez-Marquez, J. E., Barker, K., & Rocco, C. M. (2014). Stochastic measures of network resilience: applications to waterway commodity flows. Risk Analysis, 34(7), 1317.
Bompard, E., Napoli, R., & Xue, F. (2009). Analysis of structural vulnerabilities in power transmission grids. International Journal of Critical Infrastructure Protection, 2(1), 5-12.
Berle, Ø., Rice Jr., J. B., & Asbjørnslett, B. E. (2011). Failure modes in the maritime transportation system: a functional approach to throughput vulnerability. Maritime Policy & Management, 38(6), 605–632.
Bian, T., Hu, J. T. & Deng, Y. (2017). Identifying influential nodes in complex networks based on AHP. Physica A- Statistical Mechanics and its Applications, 479, 422-436.
Boutin, F., Thievre, J., & Hascoët, M. (2006). Focus-based filtering+ clustering technique for power-law networks with small world phenomenon. In SPIE Electronic Imaging/Visualization and Data Analysis, edited by R. F. Erbacher, J. C. Roberts, M. T. Gröhn, and K. Börner, volume 6060, San Jose, California.
Ducruet, C., & Notteboom, T. (2012). The worldwide maritime network of container shipping: spatial structure and regional dynamics. Global Networks, 12(3), 395-423.
Ducruet, C., Rozenblat, C., & Zaidi, F. (2010). Ports in multi-level maritime networks: evidence from the Atlantic (1996–2006). Journal of Transport Geography, 18(4), 508-518.
Ducruet, C., & Zaidi, F. (2012). Maritime constellations: a complex network approach to shipping and ports. Maritime Policy & Management, 39(2), 151-168.
Eusgeld, I., Kröger, W., Sansavini, G., Schläpfer, M., & Zio, E. (2009). The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures. Reliability Engineering & System Safety, 94(5), 954-963.
Fleming, D. K., & Hayuth, Y. (1994). Spatial characteristics of transportation hubs: centrality and intermediacy. Journal of Transport Geography, 2(1), 3-18.
Girvan, M., & Newman, M. E. (2002). Community structure in social and biological networks. Proceedings of the National Academy of Sciences, 99(12), 7821-7826.
Gol'dshtein, V., Koganov, G. A., & Surdutovich, G. I. (2004). Vulnerability and hierarchy of complex networks. Available at http://arxiv.org/pdf/cond-mat/0409298.pdf.
González Laxe, F., Jesus Freire Seoane, M., & Pais Montes, C. (2012). Maritime degree, centrality and vulnerability: port hierarchies and emerging areas in containerized transport (2008–2010). Journal of Transport Geography, 24, 33–44.
Hernández, E., Rocco, C. M., & Ramirez-Marquez, J. E. (2016). Node ranking for network topology-based cascade models – an ordered weighted averaging operators' approach. Reliability Engineering & System Safety, 155, 115-123.
Holme, P., Kim, B. J., Yoon, C. N., & Han, S. K. (2002). Attack vulnerability of complex networks. Physical Review E, 65(5), 056109.
Hu, J. T., Du, Y. X., Mo, H. M., Wei, D.J. & Deng Y. (2016). A modified weighted TOPSIS to identify influential nodes in complex networks. Physica A- Statistical Mechanics and its Applications, 444, 73-85.

Hu, Y., & Zhu, D. (2009). Empirical analysis of the worldwide maritime transportation network. Physica A: Statistical Mechanics and its Applications, 388(10), 2061-2071.

Kaluza, P., Kölzsch, A., Gastner, M. T., & Blasius, B. (2010). The complex network of global cargo ship movements. Journal of the Royal Society Interface, 7(48), 1093-1103.

Latora, V., & Marchiori, M. (2001). Efficient behavior of small-world networks. Physical review letters, 87(19), 198701.

Latora, V., &Marchiori, M. (2003). Economic small-world behavior in weighted networks. The European Physical Journal B-Condensed Matter and Complex Systems, 32(2), 249-263.

Latora, V., &Marchiori, M. (2005). Vulnerability and protection of infrastructure networks. Physical Review E, 71(1), 015103.

Laxe, F., Jesus, Seoane, M., & Montes, C. (2012). Maritime degree, centrality and vulnerability: port hierarchies and emerging areas in containerized transport (2008–2010). Journal of Transport Geography, 24, 33-44.

Lhomme, S. (2015). Vulnerability and resilience of ports and maritime networks to cascading failures and targeted attacks. In Routledge (Ed.), Maritime Networks. Spatial Structures and Time Dynamic. Routledge. Retrieved from https://hal.archives-ouvertes.fr/hal-01275157

Mishkovski, I., Biey, M., &Kocarev, L. (2011).Vulnerability of complex networks. Communications in Nonlinear Science and Numerical Simulation, 16(1), 341-349.

Newman, M. E. (2003). The structure and function of complex networks. SIAM review, 45(2), 167-256.

Newman, M. E. (2005). Power laws, Pareto distributions and Zipf's law. Contemporary physics, 46(5), 323-351.

Parand, F.A., Rahimi, H., & Gorzin M. (2016). Combining fuzzy logic and eigenvector centrality measures in social network analysis. Physica A- Statistical Mechanics and its Applications, 459, 24-31.

Rocco, C. M., & Barker, K. (2016). Stochastic Ranking of Alternatives with Ordered Weighted Averaging: Comparing Network Recovery Strategies. Systems Engineering, 19, 436-447.

Rocco, C. M., Ramirez-Marquez, J. E. & Yajure, C. (2014). A non-parametric aggregation technique for identifying critical nodes in a network, using three topology-based cascade models. 2nd International Conference on Vulnerability and Risk Analysis and Management (ICVRAM) and the 6th International Symposium on Uncertainty, Modeling, and Analysis (ISUMA), July 13-16, Liverpool, UK

Sabidussi, G. (1966). The centrality index of a graph. Psychometrika, 31(4), 581-603.

Savaresi, S. M., & Boley, D. L. (2004).A comparative analysis on the bisecting K-means and the PDDP clustering algorithms. Intelligent Data Analysis, 8(4), 345-362.

Seaton, K. A., & Hackett, L. M. (2004). Stations, trains and small-world networks. Physica A: Statistical Mechanics and its Applications, 339(3), 635-644.

Sen, P., Dasgupta, S., Chatterjee, A., Sreeram, P. A., Mukherjee, G., & Manna, S. S. (2003). Small-world properties of the Indian railway network. Physical Review E, 67(3), 036106.

Sienkiewicz, J., & Hołyst, J. A. (2005). Statistical analysis of 22 public transport networks in Poland.Physical Review E, 72(4), 046127.

Steinbach, M., Karypis, G., & Kumar, V. (2000, August). A comparison of document clustering techniques. In KDD workshop on text mining (Vol. 400, No. 1, pp. 525-526).

Taquechel, E. (2010). Layered defense: modeling terrorist transfer threat networks and optimizing network risk reduction. Network, IEEE, 24(6), 30-35.

Wang, B., Tang, H., Guo, C., Xiu, Z., & Zhou, T. (2006). Optimization of network structure to random failures. Physica A: Statistical Mechanics and its Applications, 368(2), 607-614.

Watts, D. J., &Strogatz, S. H. (1998). Collective dynamics of 'small-world' networks. Nature, 393(6684), 440-442.

Wasserman, S. (1994). Social network analysis: Methods and applications (Vol. 8). Cambridge university press.

Xu, X., Hu, J., & Liu, F. (2007). Empirical analysis of the ship-transport network of China. Chaos: An Interdisciplinary Journal of Nonlinear Science, 17(2), 023129.

Yang, Z., Bonsall, S. & Wang J. (2010). Facilitating uncertainty treatment in the risk assessment of container supply chains. Journal of Marine Engineering and Technology, A17, 23-36.

Yang, Z., Ng, A.K.Y. & Wang, J. (2014). Incorporating quantitative risk analysis in port facility security assessment. Transportation Research Part A: Policy and Practice, 59, 72-90.

Yang, Z. & Qu, Z. (2016). Development of quantitative maritime security assessment: a 2020 vision. IMA Journal of Management Mathematics, 27(4), 453-470.

Yang, Z., Wang, J. & Li, K. (2013). Maritime safety analysis in retrospect. Maritime Policy and Management, 40(3), 261-277.

Zemljič, B., & Hlebec, V. (2005). Reliability of measures of centrality and prominence. Social Networks, 27(1), 73-88.

Zio, E., & Golea, L. R. (2012). Analyzing the topological, electrical and reliability characteristics of a power transmission system for identifying its critical elements. Reliability Engineering & System Safety, 101, 67-74.

Zio, E., Golea, L. R., & Rocco S, C. M. (2012). Identifying groups of critical edges in a realistic electrical network by multi-objective genetic algorithms. Reliability Engineering & System Safety, 99, 172-177.

Zwicker, W S. (1991). The voters' paradox, spin, and the Borda count. Mathematical Social Sciences, 22(3), 187-227.