

PAPER • OPEN ACCESS

Robustness of maritime network along the Maritime Silk Road based on trajectory data

To cite this article: Yanxin Xie 2019 *IOP Conf. Ser.: Earth Environ. Sci.* **310** 022034

View the [article online](#) for updates and enhancements.



IOP | ebooks™

Bringing you innovative digital publishing with leading voices to create your essential collection of books in STEM research.

Start exploring the [collection](#) - download the first chapter of every title for free.

Robustness of maritime network along the Maritime Silk Road based on trajectory data

Yanxin Xie^{1,*}

¹College of Geomatics, Shandong University of Science and Technology, Qingdao 266590, China

*Corresponding author: xyx112113@163.com

Abstract. Most of the current research on the robustness of the maritime network is based on container liners, ignoring the diversity of maritime trade. Based on the 2014 AIS trajectory data, this paper constructs the maritime network of three cargo ships of container, tanker and bulk along the MSR. The author uses two strategies of random attack and deliberate attack to analyze the changes of three networks under different attack strategies. The study finds: (1) The maritime network that is constructed based on the real cargo ship AIS trajectory more fully reflects the changes in the maritime trade route of the MSR. (2) The dry bulk maritime network is the most robust, the tanker maritime network is second, and the container maritime network is the most vulnerable. (3) In the deliberate attack, the container maritime network is extremely vulnerable, and the collapse domain of the tanker maritime network is short. Once the tanker network begins to collapse, it will quickly fail. The research results can provide decision-making basis for a comprehensive understanding of the MSR shipping trade, port investment planning, route optimization.

1. Introduction

The “21st Century Maritime Silk Road” (MSR) is an emerging trade path connecting China to the world under the ever-changing global political and trade pattern. At present, the MSR coverage continues to expand, accounting for more than 35% of global merchandise trade and about 30% of global GDP [1]. Maritime trade has a major impact on global economic development and international political exchanges, and is also highly vulnerable to external factors such as geopolitics, oil price fluctuations and natural disasters [2]. Therefore, quantitatively assess the robustness of the MSR maritime network has important practical significance for improving shipping efficiency, optimizing routes and strengthening investment along ports.

In complex network research, robustness refers to the ability of a network to maintain its function under random conditions or deliberate attacks on nodes or edges in the network [3-4]. There are also studies called reliability. The level of robustness reflects the strength of anti-interference ability. This paper observes the changes of various indicators of MSR maritime network through different strategies of network attacks, and compares and analyzes the differences in anti-interference ability of different types of shipping networks. Research on network robustness is widely involved in many fields such as road traffic networks, aviation networks, wireless networks, power networks, and virus propagation networks [5-7]. In the related research of the maritime network, Woolleymeza et al. [8] compared the air transport network, and believed that the maritime network showed better robustness in response to deliberate attacks. Wang et al. [9] used the data of the world’s major container liner



companies in 2004 and 2014 to analyze and found that under the deliberate attack, the global container maritime transport network has become more and more fragile in the past 10 years. By constructed the MSR container maritime network, Wu et al. [10] revealed the critical point of the network began to collapse and completely collapse under deliberate attacks, and accordingly pointed out the key trunk ports that need to be protected. Combined with geographical features, it is found that the Malacca Strait, the Taiwan Strait, the Mandab Strait and the Suez Canal have the most significant impact on the vulnerability of the network.

Most of the research carried out mainly focuses on container liner data, while maritime trade involves different types of goods. In addition to container transportation, crude oil and dry bulk transportation are also important components of current maritime trade [11]. In addition, different ports have different functional positioning and cargo differentiation, and this difference has an important impact on the global marine transportation network structure. Therefore, based on the AIS trajectory data of marine vessels, this paper constructs the container maritime network, tanker maritime network and bulk maritime network along the MSR. Combined with the complex network method, the robustness of the three maritime networks is quantitatively evaluated, in order to provide decision-making reference for port investment and route optimization.

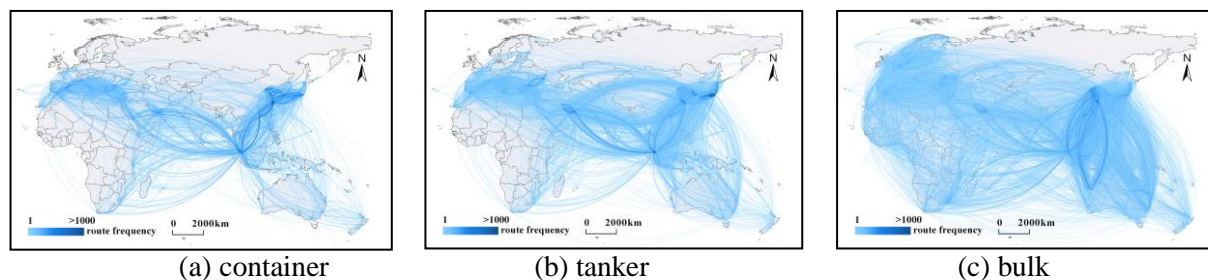


Fig. 1. The maritime network structure of Maritime Silk Road

2. Study areas and data

This paper refers to the “BELT AND ROAD PORTAL” network and selects 65 relevant countries along the MSR. The AIS trajectory of the shipping vessel along the MSR in 2014 was used for analysis, mainly including the shipping sub-network of three cargo ships of container, oil tanker and dry bulk. This paper extracts the ship's OD record based on the AIS trajectory, and combines the global port index data to finally obtain 157,225 container OD data, 320,310 oil tanker OD data, and 218,070 dry bulk OD data. Fig.1 shows three maritime network structure diagrams based on OD data.

Compared with the previous research on the shipping network based on container liners [10], the maritime network constructed based on the AIS trajectory is more comprehensive in terms of ports and routes. In addition to regular routes, it also contains a large number of irregular routes, block trades, and low-priced goods transport business. These can fully and effectively reflect the trade changes in the shipping along the Maritime Silk Road.

3. Evaluation index of Maritime network robustness

3.1 Maritime network structure analysis

It is generally believed that when the degrees of all nodes in a network are subject to a power-law distribution, the network has a scale-free characteristic. The scale-free network simultaneously exhibits robustness against random failures and vulnerability to deliberate attacks [12]. As shown in Fig.2, in the double logarithmic coordinate system, the three types of maritime networks are subject to a power-law distribution and belong to a scale-free network.

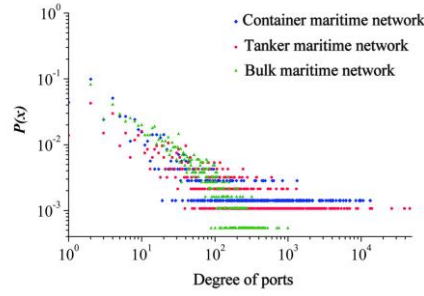


Fig. 2. Degree distribution of maritime networks

This paper uses a set of topological feature metrics from node to network to quantitatively describe the robustness of the maritime network. The MSR maritime network G is expressed as:

$$G = (N, E) \quad (1)$$

N is a collection of port nodes in the maritime network, and E is a collection of maritime trade connections between ports.

3.2 Metrics of port importance

In this paper, two indicators, node degree and betweenness centrality, are used to determine the importance of port nodes in the entire maritime network. The port degree d_i represents the number of edges connected to the port node i . The calculation formula of port degree is:

$$d_i = \sum_{j \in N, j \neq i} e_{ij} \quad (2)$$

N is a collection of all ports. i, j represent two different port nodes in the set N , e_{ij} represents the trade connection between the port i and the port j .

Port betweenness centrality $C_{(b,i)}$ refers to the proportion of the shortest path through port node i in the shortest path of any two nodes in the maritime network. Its calculation formula is:

$$C_{(b,i)} = \frac{1}{(n-1)(n-2)} \sum_{j \neq i \neq k} \frac{n_{ijk}}{n_{jk}} \quad (3)$$

n_{jk} represents the shortest number of paths between ports j and k ; n_{ijk} represents the number of port i passing through the shortest path between ports j and k . n is the total number of port nodes included in the entire maritime network.

3.3 Metrics of network complexity

Changes in ports within the maritime network and the impact of external factors (such as supply chain performance, transport service model adjustment, and hinterland accessibility) often cause dynamic changes in the structural characteristics of the maritime network. This paper selects three commonly used metrics, average shortest path length, clustering coefficient and network fragmentation.

L is the relative average shortest path length, is the ratio of the average shortest path length l to the network diameter D . It can be calculated as follows:

$$L = \frac{l}{D} \quad (4)$$

D is the network diameter. l refers to the average of the shortest path lengths between all nodes in the maritime network.

$$l = \frac{1}{n(n-1)} \sum_{i \in N} \sum_{j \neq i \in N} d_{ij} \quad (5)$$

C refers to the average of the clustering coefficients of all port nodes in the maritime network, and its calculation formula is:

$$C = \frac{1}{N} \sum_{i \in N} C_i \quad (6)$$

Where C_i represents the clustering coefficient of the port i , E_i represents the number of edges

actually connected to the port, and k_i is the neighbor node of the node i .

$$C_i = \frac{E_i}{k_i(k_i-1)/2} \quad (7)$$

The degree of fragmentation of the maritime network S can be measured by the relative size of the largest connected component in the network. Its calculation formula is:

$$S = \frac{n_s}{n} \quad (8)$$

Where n_s represents the number of nodes included in the largest connectivity component in the current network; n is the number of original maritime network port.

4. Robustness of MSR maritime networks

This paper uses random attack and deliberate attack to analyze the change process and robustness of the maritime network structure of the MSR. For three different types of maritime networks, attack the maritime network according to different attack strategies. Delete one port node and the connected edge each time, and count the values of the L , C , and S indicators of the current maritime network until all nodes was deleted and the maritime network was completely invalid.

4.1 Simulated attack

Fig.3, Fig.4, and Fig.5 show the changes in the different types of MSR maritime networks structure, including random attacks, degree-based deliberate attacks, and betweenness-based deliberate attacks. The X-axis represents the degree of attack (the ratio of the number of removed nodes to the total number of nodes in the original network). The Y-axis represents the structural metrics (relative average shortest path length, clustering coefficient, and fragmentation) of the current maritime network.

As shown in Fig.3, under the continuous random attack, the L of the three types of maritime networks is generally stable as the degree of attack increases. Small fluctuations in the middle process is due to the removal of certain ports. The change of the network C is relatively stable, and S shows a slowly decreasing trend as the degree of attack increases.

As shown in Fig.4, compared with the random attack mode, under the degree-based deliberate attack, the structural changes of the three maritime networks show obvious differences. L has a tendency of zigzag up and down during the first half of the attack, the change is extremely unstable, and the latter half then decreases sharply. C , with the degree of attack, first and then slow down slowly. S shows a sharp decline and the network quickly collapses. Among them, the change of the container network is most sensitive in the deliberate attack mode based on the node degree; the tanker maritime network is second, and the structural change of the bulk maritime network is relatively stable.

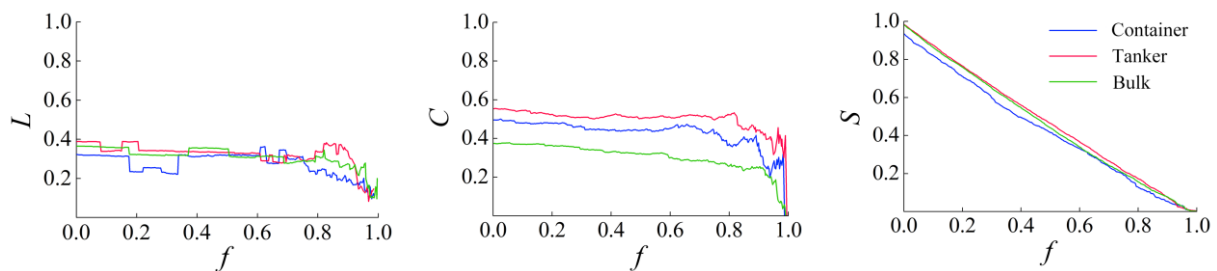


Fig. 3. Maritime network structural changes under random attacks

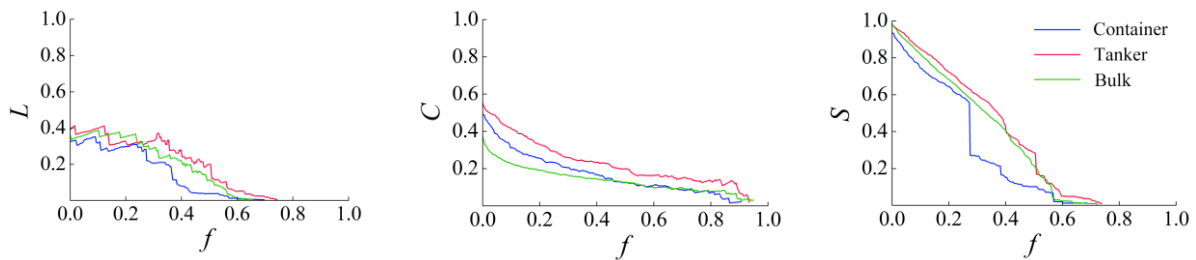


Fig. 4. Maritime network structural changes under degree-based deliberate attacks

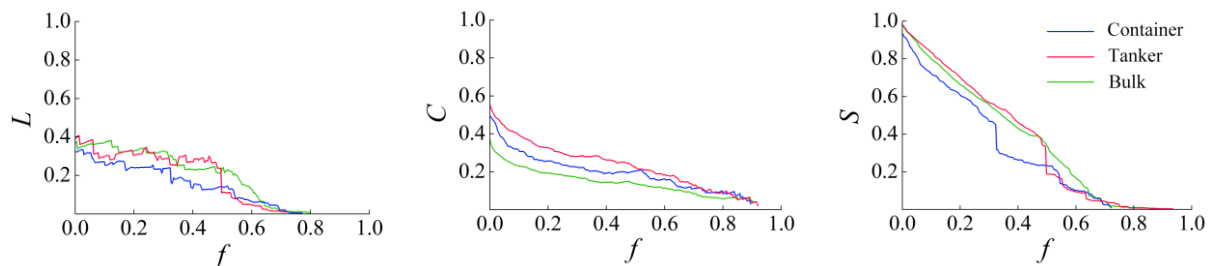


Fig. 5. Maritime network structural changes under betweenness-based deliberate attacks

As shown in Fig.5, the structural changes of the maritime network are presented under the betweenness-based deliberate attack mode. It can be seen from the figure that the betweenness-based deliberate attack has less damage to the maritime network of the MSR than the degree-based deliberate attack. L exhibits up and down fluctuations during most of the attack period. Similar to the node-based attack, C shows a rapid and slow decline with the degree of attack. S shows a sharp decline, and the degree of attack when the network crashes is greater than the degree of deliberate attack based on degree.

Under the two deliberate attack modes, L , C , and S all showed the same change pattern. Among them, the bulk maritime network is more robust than the tanker maritime network, the tanker maritime network is more robust than the container maritime network, and the container maritime network is the most vulnerable.

4.2 Half-life of networks

Under the deliberate attack strategy, the attack strength corresponding to the change rate of a certain characteristic index of the maritime network which reaches 50% of the maximum value (that is, the network completely fails) is called the half-life of networks, represented by G_s . And s is a metric. It is generally believed that a 50% ratio, that is, the median value of the network failure and complete failure, is the most reasonable choice.

As shown in Fig.6, under the deliberate attack of the two modes, the half-life of the container maritime network is the smallest, and the half-life of the tanker maritime network is the largest. It can be seen from the comparison of different indicators that the change of the aggregation coefficient C is the most sensitive, that is, the ability of local maritime transport is rapidly declining during the attack. The speed of L attenuation is relatively slow, that is, the overall transportation efficiency of the marine network is relatively stable. In addition, the tanker and bulk maritime networks involve more ports than container network. The overall network trade connection is closer so it's more secure in responding to cyber attacks.

4.3 Crash domain of networks

From the experimental results of the simulated attack, it can be known that the MSR maritime network is resilient to different modes of attack. Identifying the collapse threshold of the maritime network contributes to the marine transportation warning. For maritime networks, when the maximum size of

the largest connectivity components decreases sharply for the first time, it can be determined that the network at this time begins to collapse. The relative size of the largest connectivity component drops below 10%, and it can be determined that the network has collapsed into many sub-networks [10]. It can be seen from Fig.7 that for the random attack, all three types of maritime networks show good robustness. The smallest container maritime network was also severely damaged and crashed when 84.13% of the ports failed. For deliberate attacks, the MSR maritime network is less robust. In the case of degree-based attacks, it is more likely to cause the maritime network to start to collapse. In the case of betweenness-based attacks, it is easy to cause the overall failure of the network. The container network has the longest crash domain, the bulk network, and the tanker network's crash domain is the shortest.

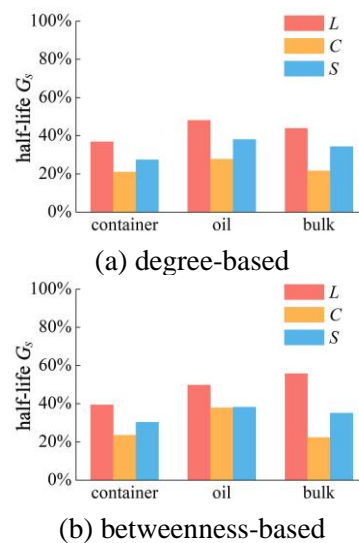


Fig. 6. Half-life of different types of maritime network structures under deliberate attacks

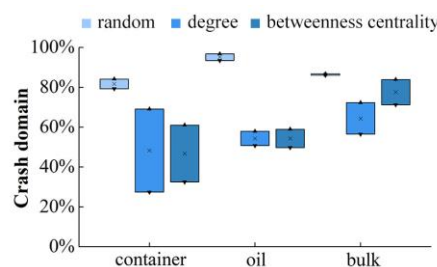


Fig. 7. Crash domain for different types of maritime networks

5. Conclusion

This paper uses the AIS data of marine transport ships in 2014 to construct the MSR maritime transportation networks, and quantitatively analyzes the structural robustness of the three types of maritime networks: container, tanker and bulk cargo. And we obtain the following conclusions: (1) The maritime network based on the real cargo ship AIS trajectory more fully reflects the changes in the maritime trade route of the MSR. (2) The bulk maritime network is the most robust, followed by the tanker maritime network, and the container maritime network is the most vulnerable. (3) In the deliberate attack, the container maritime network is extremely vulnerable. The tanker maritime network will quickly fail once it begins to collapse. However, maritime trade is a dynamic process that is constrained by port performance, geopolitics, hinterland economy, and climatic conditions. Therefore, future research will further integrate more influencing factors to improve the maritime robustness assessment system.

References

- [1] L H Wang, Y Zhu, C Ducruet, et al. From hierarchy to networking: the evolution of the “twenty-first-century Maritime Silk Road” container shipping system. *J. Transport Reviews*. **38**, 4 (2018)
- [2] H C Yu, Z X Fang, F Lu, et al. Impact of oil price fluctuations on tanker maritime network structure and traffic flow changes. *J. Applied Energy*. **237**, (2019)
- [3] M Jalili. Error and attack tolerance of small-worldness in complex networks. *J. Journal of Informetrics*. **5**, 3 (2011)
- [4] L X Tian, Y Huang, G G Dong, et al. Robustness of interdependent and interconnected clustered networks. *J. Physica A: Statistical Mechanics and its Applications*. **412**, 120-126 (2014)
- [5] A Socievole, R F De, C Scoglio, et al. Assessing network robustness under SIS epidemics: The relationship between epidemic threshold and viral conductance. *J. Computer Networks*. **103**, 196-206 (2016)
- [6] O Lordan, J M Sallan, N Escorihuela, et al. Robustness of airline route networks. *J. Physica A: Statistical Mechanics and its Applications*. **445**, 18-26 (2016)
- [7] O Cats, E Jenelius. Planning for the unexpected: The value of reserve capacity for public transport network robustness. *J. Transportation Research Part A: Policy and Practice*. **81**, 47-61 (2015)
- [8] O Woolley-Meza, C Thiemann, D Grady, et al. Complexity in human transportation networks: a comparative analysis of worldwide air transportation and global cargo-ship movements. *J. European Physical Journal B*. **84**, 4 (2011)
- [9] N Wang, L L Dong, N Wu, et al. The change of global container shipping network vulnerability under intentional attack. *J. Acta Geographica Sinica*. **71**, 2 (2016)
- [10] D Wu, N Wang, A Q Yu, et al. Vulnerability and risk management in the Maritime Silk Road container shipping network. *J. Acta Geographica Sinica*. **73**, 6 (2018)
- [11] P Kaluza, A Kölzsch, M T Gastner, et al. The complex network of global cargo ship movements. *J. Journal of the Royal Society Interface*. **7**, 48 (2010)
- [12] H Jeong, B Tombor, R Albert, et al. The large-scale organization of metabolic networks. *J. Nature*. **407**, 6804 (2000)