Mathematics and Computer Science
2022; 7(3): 48-52
http://www.sciencepublishinggroup.com/j/mcs
doi: 10.11648/j.mcs.20220703.13
ISSN: 2575-6036 (Print); ISSN: 2575-6028 (Online)

Research on the Vulnerability of China-Europe Railway Express Network

Wang Nana*, Gao Xinxin, Wang Xueqing

School of Liberal Studies, Liaoning University of International Business and Economics, Dalian, China

Email address:
wangnana124@aliyun.com (Wang Nana), 2239977381@qq.com (Gao Xinxin), 1983208220@qq.com (Wang Xueqing)
*Corresponding author

To cite this article:
Wang Nana, Gao Xinxin, Wang Xueqing. Research on the Vulnerability of China-Europe Railway Express Network. *Mathematics and Computer Science*. Vol. 7, No. 3, 2022, pp. 48-52. doi: 10.11648/j.mcs.20220703.13

Received: April 13, 2022; **Accepted**: May 12, 2022; **Published**: May 19, 2022

Abstract: In order to study the vulnerability of the European express train transport network, statistics were made on the countries and cities along the route. The two methods of intentional attack are to study the changes of the network characteristic values, such as the average degree of the network, the proportion of isolated nodes, the average path length, and the network efficiency. Under the deliberate attack, the node average degree, aggregation coefficient, network efficiency, and average path length of the China-Europe train network decrease rapidly with the increase of the attack ratio and decrease to 0. Under random attack, the average node degree, network efficiency, and average path length of the network show a slow decreasing trend with the increase of the attack ratio, and the aggregation coefficient increases slowly and then decreases. The isolated node is no longer connected to other nodes under the deliberate attack and random attack, so the attacked node is the isolated point, which increases the cardinality of the isolated node. The research shows that the China Railway Express network is relatively strong when subjected to random attacks, and relatively vulnerable when subjected to deliberate attacks. At the same time, it is found that some nodes in the China Railway Express play an important role in the connectivity of the network.

Keywords: China-Europe Railway Express, Complex Networks, Vulnerability, Connectivity, Damage Resistance

1. Introduction

The China-Europe Express runs according to fixed trains, fixed routes, fixed schedules and full schedules, and runs international intermodal trains such as containers between China and Europe and countries along the Belt and Road. The China-Europe express train has formed a basic pattern characterized by three major channels, four major ports, five directions and six major lines. Studying the vulnerability of the European train network and finding the weak links of the network is of great significance to the trade cooperation of countries along the route.

Wu Di in view of the vulnerability of the container shipping network of the Maritime Silk Road, the Silk Road network is constructed, and the network structure analysis of the Silk Road network is analyzed by using complex network theory, and the changes in the characteristics of network connectivity are analyzed by using two attack methods: random attack and deliberate attack, and points out which areas are weak offensive areas, and proposes corresponding countermeasures, which is of great application value [1].

Xu Yingming in view of the unobstructed passage of China-Europe express trains, that is, the transportation situation of fast at both ends and slow in the middle, he proposed countermeasures to improve the efficiency of traffic and improve the smooth passage of the Belt and Road [2].

Wu Shan in view of the impact of network vulnerability on shipping trade, the theory and method of complex networks are used to explore the vulnerability of global maritime networks, and studies have shown that deliberate attacks are more obvious than random attacks under the vulnerability of networks, and network efficiency declines faster [3]. Duan Jiayong in view of how to accurately predict the weak links of the network, the analysis method of the fragile links of the complex network is designed, and the effectiveness of the method is verified by taking a railway network as an example. Experiments show that the method can more accurately infer the weak links in the network [4]. Wang Nuo in view of the changing trend of vulnerability of the global container

shipping network, the network stress test method is proposed by using complex network theory, taking 2004 and 2014 as an example, the nodes and corresponding edges are gradually deleted according to the size of the node degree in the proportion of 1%-10%, and the changes of quantitative indicators are analyzed, and the research results have a reference effect on deepening the research of port geography [5]. Ji Mingjun under the initiative of the Belt and Road Initiative, in view of the particularity of the China-Europe express train transported by the New Eurasian Land Bridge, the problems existing in the logistics park were analyzed, and different logistics nodes were proposed to build differentiated logistics parks and strengthen the cooperation of logistics parks, thereby promoting the smooth operation of the new Eurasian continent [6]. Literature the study analyzes the reliability of port security in the context of terrorist attacks [7-10].

Albret first studied the invulnerability of complex networks in 2000, mainly concerned with the impact of topology on the invulnerability of complex networks, and concluded that the network has strong invulnerability to targeted attacks [11].

References deliberately attack the transportation network and power network by using the height number and high betweenness, and then analyze the changes of various network indicators to determine the vulnerability of each part [12-15].

In this paper, the trains of countries and cities along the route are constructed, and the container network of China-Europe express trains is constructed, and the changes in the average degree of the network, the proportion of isolated nodes, the average path length, and the network efficiency of the network are studied in two ways, namely random attacks and deliberate attacks.

2. Network Building

This paper counts 63 central European train information, each of which includes departure point, arrival point, departure city, transit country or city.

The model of China-Europe express train network is as follows:

1) Each city is 1 node.
2) Transport between cities is round-trip, so the network is abstracted into a directionless network without regard to the direction of the edges.

China Railway Express Network is shown in Figure 1 below:

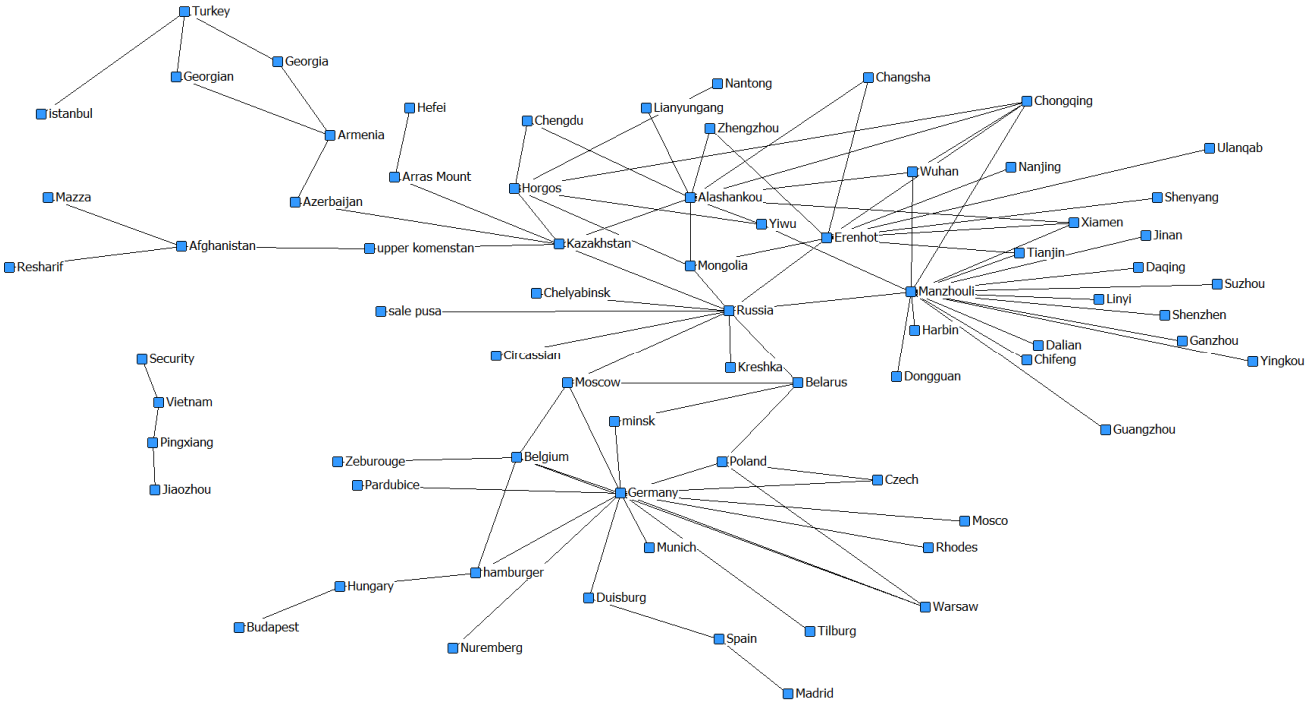

Figure 1. *China Railway Express Network.*

2.1. Average Node Size of the Network

The concept of network average refers to the average node degree of all nodes in the network, which is the average of all nodes in the network when the main channel of the China-Europe express train is attacked. In fact, when the main channel of the network is attacked, the nodes and edges of the network are also reduced, the average degree of network nodes also changes, the greater the average degree of change rate, the more sensitive the network means that the more vulnerable, set N as the total number of nodes in the China-Europe train network, K is the average degree of the Central European train network, k_i is the node degree of the node i, then

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

2.2. Proportion of Orphaned Nodes

Orphaned nodes are the proportion of nodes to which they have no edges attached. When a site in a network is attacked and the network transportation cannot operate normally, which in turn affects the size and connectivity of the entire network, the proportion of isolated nodes is:

$$\Delta N = \left(1 - \frac{N^*}{N}\right) \times 100\% \tag{2}$$

2.3. Average Path Length

The average path length refers to the average of the shortest paths between all node pairs in the network, and it is also an important indicator of network vulnerability. In general, when the network is attacked, but the network has not yet caused the network to fragment, the average path length can reflect the average degree of separation between nodes, set d_{ij} as the shortest path length between nodes i and node j, that is, the calculation formula of the average path length of the network L is:

$$L = \frac{2}{N(N-1)} \sum_{i=1}^{N} \sum_{j=i+1}^{N} d_{ij} \tag{3}$$

2.4. Network Efficiency

Network efficiency refers to the sum of the efficiency of all nodes, it reflects the difficulty of network transportation, the higher the network efficiency indicates that the better the connectivity of the network, set h_{ij} is the reciprocal of distance d_{ij}, E is the network efficiency, then

$$E = \frac{1}{N(N-1)} \sum_{i=1}^{N} \sum_{j=1(j \neq i)}^{N} h_{ij} \tag{4}$$

2.5. Aggregation Coefficient

The aggregation factor refers to the average probability of a connection between two nodes connected to the same node in a network, which reflects the degree of aggregation of the network. When the nodes in the network are attacked, the network becomes loose, so that the aggregation coefficient of the network also decreases, and the aggregation coefficient of the nodes is set:

$$C_i = \frac{2M_i}{k_i(k_i - 1)}, i = 1, 2, 3, \cdots, N \tag{5}$$

In Equation (5): M_i is the number of edges that exist between the neighboring nodes of node i.

The aggregation coefficient C of the network is calculated as follows:

$$C = \frac{1}{N} \sum_{i=1}^{N} C_i$$

3. Vulnerability Analysis of Network Nodes

Deliberate attacks and random attacks are the main way to test the vulnerability of the network, random attack refers to the deletion of network nodes with a certain probability to simulate the impact of random events on The China-Europe train. Deliberate attack refers to the deletion of nodes in the network according to the number of nodes from the largest to the smallest to study the impact on the China-Europe train. In order to quantify the vulnerability of the network, this paper gradually simulates random attacks and deliberate attacks at a rate of 1.3%, and calculates the changes in network characteristics such as average node size, aggregation coefficient, isolated node ratio, network efficiency, and average path length of the network when attacked.

As can be seen from the following figure, when a network is subjected to a random attack, the average node size, aggregation coefficient, proportion of isolated nodes, network efficiency, and average path length of the network change more slowly. When the network is deliberately attacked, the average node degree, aggregation coefficient, orphaned node ratio, network efficiency, and average path length of the network change greatly, which indicates that the network is relatively strong when it is randomly attacked. Networks are vulnerable when they are deliberately attacked.

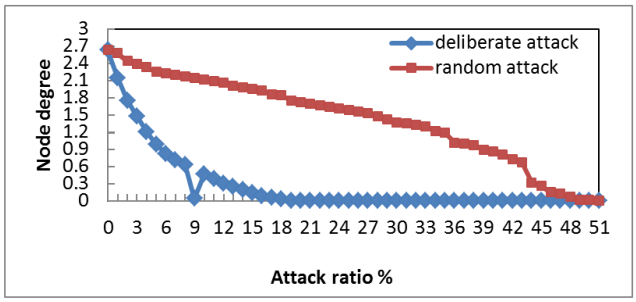

Figure 2. *Node degree.*

As can be seen from Figure 2 below, when the network suffers random attacks, the average node degree of the network changes slowly. When the network is attacked deliberately, the average node degree of the network varies greatly.

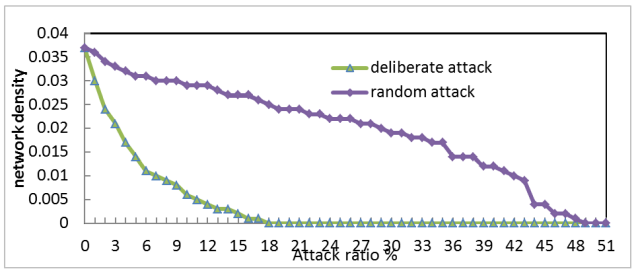

Figure 3. *Network density.*

As can be seen from Figure 3 above, when the network is subjected to random attacks, the network efficiency of the network changes slowly. When the network is attacked deliberately, the network efficiency of the network varies greatly. When the attack ratio is 18%, the network density of the network is zero.

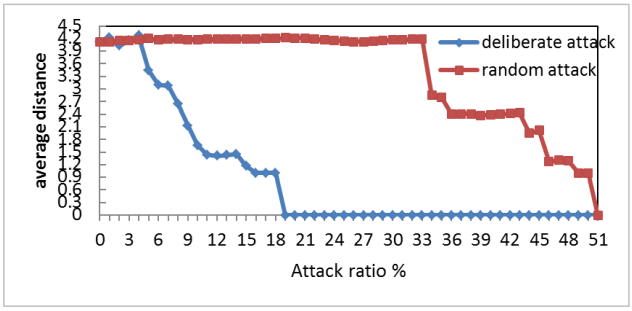

Figure 4. *Average distance.*

As can be seen from Figure 4 above, when the network is subjected to random attacks, the average path length beginsto change little, and when the attack ratio is 33%, there is a significant decrease. When the network is attacked deliberately, the average path length of the network varies greatly

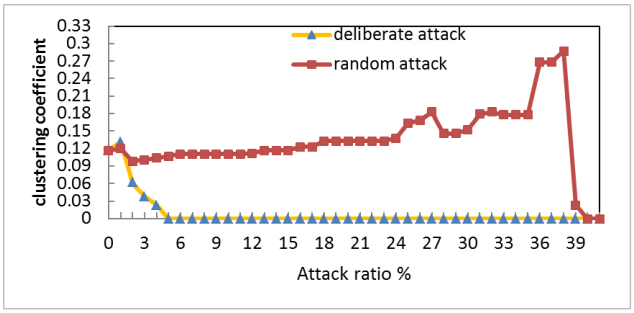

Figure 5. *Clustering coefficient.*

As can be seen from Figure 5 above, when the network is subjected to random attacks, the variation of the aggregation coefficient of the network starts relatively slowly, and then drops rapidly when the attack ratio reaches 37%. When the network is attacked deliberately, the aggregation coefficient of the network varies greatly. When the attack ratio reaches 5%, the aggregation coefficient is zero.

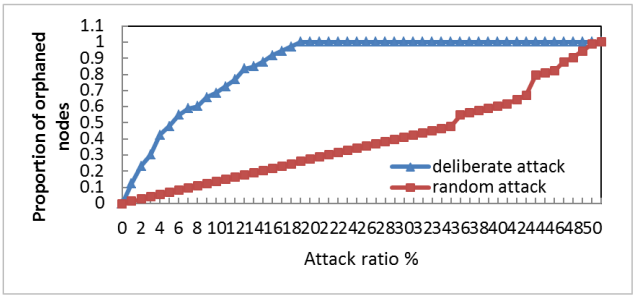

Figure 6. *Proportion of orphaned nodes.*

As can be seen from Figure 6 above, when the network suffers random attacks, the proportion of isolated nodes in the network changes slowly. When the network is attacked deliberately, the aggregation coefficient of the network varies greatly. When the attack ratio reaches 20%, the network is basically in a scattered state.

As can be seen from the above figure, under the deliberate attack, the node average, aggregation coefficient, network efficiency, and average path length of the China-Europe express train network decrease rapidly with the increase of the attack ratio and decrease to 0. Under random attacks, the node average, network efficiency, and average path length of the network show a slow decreasing trend with the increase of the attack proportion, and the aggregation coefficient slowly increases and decreases. Orphaned nodes are no longer connected to other nodes under deliberate and random attacks, so the attacked nodes are isolated points, which increases the cardinality of orphaned nodes.

4. Conclusion

This paper counts the operating lines of China-Europe express trains, using complex network theory to study the vulnerability of European trains, the study shows that the network is relatively strong under random attacks, and the network is more vulnerable under deliberate attacks, while some nodes in China-Europe trains play an important role in network connectivity. At the same time, some nodes in the China Railway Express play an important role in the connectivity of the network.

Acknowledgements

Thanks for to the support of Ph.D. scientific research initiated and funded projects (2021XJLXBSJJ03), Research Project Plan of China Society of Logistics and China Federation of Logistics and Purchasing (2022CSLKT3-218) and Liaoning Province General Higher Education Undergraduate Teaching Reform Research General Project (2021SJJGYB03).

References

[1] WU Di, WANG Nuo, YU Anqi, GUAN Lei. Vulnerability and risk management in the maritime silk road container shipping network [J]. Acta Geographica Sinica. 2018, 73 (6): 1133-1148.

[2] Xu Yingming, Xing Lizhi, Dong Xianlei. Research on the trade channel of China-Europe trains under the Belt and Road Initiative [J]. International Trade, 2019, 2: 80-86.

[3] WU Shan, HAN Xiaolong, LIU Chanjuan, et al. Vulnerability analysis of global container shipping network based on complex network. Computer Engineering and Applications, 2018, 54 (15): 249-254.

[4] DUAN Jiarong, ZHENG Hongda. Vulnerability analysis method for complex networks based on node importance [J]. Control Engineering of China, 2020, 27 (4): 692-696.

[5] WANG Nuo, DONG Lingling, WU Nuan, YAN Huakun. The change of global container shipping network vulnerability under intentional attack [J]. Acta Geographica Sinica. 2016, 71 (2): 293-303.

[6] JI Mingjun, LIU Shuangfu, GUO Xinghai. A study on the development planning of logistics parks along new eurasian land bridge [J]. Railway Transport and Andeconomy, 2019, 41 (2): 94-99.

[7] Yang Z L, Adolf N, Wang J. A new risk quantification approach in port facility security assessment [J]. Transportation Research Part A, 2014, 59: 72-90.

[8] Yang Z L, Adolf N, Wang J. Prioritising security vulnerabilities in ports [J]. International Journal of Shipping and Transpor tLogistics, 2013, 5 (6): 622-636.

[9] Talas R, Menachof D. Using portfolio optimisation to calculate the efficient relationship between maritime port security residual risk and security investment [J]. International Journal of Shipping and Transport Logistics, 2014, 6 (3): 314-338.

[10] Germond B. The geopolitical dimension of maritime security [J]. Marine Policy, 2015, 54: 137-142.

[11] A lbertR, Jeong H, BarabásiA-L. Error and attack tolerance of complex networks [J]. Nature, 2000, 406: 378-382.

[12] Zhao S C. Study on Reliability of Urban Public Transit Network Based on Complex Network Theory [J]. China Safety Science Journal, 2013, 23 (4): 108-112.

[13] Huang D R, Shen L B, Zhao L. Vulnerability Analysis of Urban Road Network Based on Complex Network Theory [J]. Journal of Chongqing Jiaotong University (Natural Science), 2015, 34 (1): 110-115.

[14] Liu D C, Ji X P, Wang B, et al. Topological Vulnerability Analysis and Countermeasures of Electrical Communication Network Based on Complex Network Theory [J]. Power System Technology, 2015, 39 (12): 3615-3621.

[15] Jiang X Y, Ji X, Huang J. Vulnerability Analysis of Shipboard Power Network Based on Complex Network Theory [J]. Ship Science and Technology, 2014, (8): 46-52.