城市轨道交通网络脆弱性分析

Vulnerability Analysis of Urban Rail Transit Networks

赵宇晗 孙健
Yuhan ZHAO Jian SUN
船舶海洋与建筑工程学院
School of Naval Architecture, Ocean and Civil Engineering

摘要

随着社会经济的发展和城市人口的急剧增加，城市轨道交通逐步成为保证居民顺畅出行和解决交通拥堵问题的有效手段。近年来，城市轨道交通快速发展，其运营的安全性和稳定性成为我们必须要面对的一个课题。本课题基于复杂网络理论和图论理论，以上海地铁为主要研究对象，并结合对台北地铁、东京地铁的相关对比研究，讨论城市轨道交通网络的拓扑脆弱性和功能脆弱性。研究表明：城市轨道交通网络对于随机攻击具有一定鲁棒性，但是对于最大度节点攻击和最高介数节点攻击具有很大的脆弱性；东京地铁网络具有较好的网络拓扑结构，兼顾网络可靠性和建设成本经济性两方面的考虑，且具备较好的运输功能及 OD 连通性。这将为城市轨道交通网络的规划和建设提供参考。

关键词：脆弱性，城市轨道交通网络，复杂网络理论，蓄意攻击

Abstract

Compared with road transport, urban rail transit networks, such as metros, light rail and regional railways have provided superior performance. Nevertheless, the security and stability operations become a topic that we have to face. In this paper, topological and functional vulnerability of urban rail transit networks are analyzed based on complex network theory and graph theory. Urban rail transit networks are constructed and several basic parameters are proposed to investigate general characteristics of rail transit networks. Shanghai Metro is taken as the study object to explore the vulnerability of a typical urban rail transit network. Vulnerabilities of different urban rail transit networks, namely Shanghai Metro, Taibei Metro and Tokyo Metro are compared to explore the most reliable network geometry. It is shown in the paper that urban rail transit network is quite robust to random attacks, but it is vulnerable to the largest degree node-based attacks and the highest betweenness node-based attacks. Tokyo Metro is not only robust for critical-station attacks, but also more economical in constructing other less critical stations than Shanghai Metro and Taibei Metro. It possesses the best transport ability under malicious attacks among the three metros and is much more robust to the largest degree node-based attacks in OD connectivity. This research could provide both theoretical significance and practical significance to the study of rail transit networks.

Key words: vulnerability, urban rail transit network, complex network theory, malicious attacks

1 Introduction

1.1 Background

In recent years, cities are expanding with a rapid increase in population. Traditional public transport and private vehicles have posed serious problems on city roads, such as congestions and pollution, etc. Compared with road transport, urban rail transit networks, such as metros, light rail and regional railways have provided superior performance. Nevertheless, the security and stability operations become a topic that we have to face. Network failures, outburst of passenger flows, natural disasters and terrorist activities may cause breakdown of stations or lines, which would affect the overall efficiency of the rail networks. Only in Shanghai, for example, on October 27th 2007, power failures led to the breakdown of three subway lines; on December 22th 2009, a power blackout of Line 1 direct resulted in a two-train crash; on September 27th 2011, a rear-end accident on Line 10 happened between Yuyuan Garden and Laoximen stations; more commonly, on September 14th 2013, water intrusion caused the signal failure of Line 2 and a large number of passengers were stranded at the stations. Compared with road network accidents, rail accidents not only cause traffic delays of the incident line, but also have a wider impact on other stations of the system, which generate a greater social impact.

1.2 Literature review

Urban rail transit network has a history of more than 150 years; therefore, traditional literatures are abundant. Musso and Vuchic [1] notably investigated the geometric characteristics of metro networks. Their research defined the most important measures, indicators, and characteristics of geometric forms which improved the empirical methods used in metro network planning and analysis. More recently, Zhang and Zhao [2] comprehensively introduced the major urban rail transit systems in the world, which provided basic information for the rail transit network planning and construction. Vuchic [3] systematically introduced the metro network operations, planning and economics. Topics such as transit line capacity, rail transit station location, transit system planning, transit fare, etc. were all covered in the book.

In recent 10 years, graph theory and complex network theory have been applied to the urban rail transit networks, but research from this specific approach remained relatively limited. Latora and Marchiori [4] gave insights on the general characteristics of real transportation networks and notably identified the small-world features in the Boston subway network. Seaton and Hackett [5] calculated the clustering coefficient, path length and average vertex degree of the Boston and Vienna networks, and investigated the effect of architecture on the small-world properties. Vragović et al. [6] measured and compared the network efficiencies of Madrid, Barcelona and Boston subway networks and categorized these systems as declustered networks. Angeloudis and Fisk [7] defined the subway systems as complex networks and analyzed 20 networks constructed from the world’s largest subways. They discovered that the urban rail transit networks possessed the characteristics of high connectivity but low maximum vertex degree. Lee et al. [8] analyzed statistical properties and topological consequences of the rail transit network system, and further studied the passenger flows on the system. Raveau et al. [9] presented a route choice model for public transit networks that incorporated variables related to network topology. This study significantly improved the explanatory and predictive ability of existing route choice specifications.

According to the above mentioned literatures, the urban rail transit network is a very complex system; therefore, much attention has been paid to the prevention of network failures and system disruptions so far. Zhao [10] studied the operational safety and reliability of urban mass transit system. Beroggi (2000) provided an integrated approach to develop a safety concept for underground systems. Canós and Zulueta [11] applied hypermedia technology to improve safety in underground metropolitan transportation and to reduce emergency response time. Xu et al. [12] designed and implemented an emergency management system of urban rail transit network based on workflow modeling.

Network science has also been applied to the analysis of reliability and safety of the urban rail transit networks. Santiago del Río et al. [13] analyzed the resilience capabilities of underground systems and calculated the amount of backup capacity required to recover from system failures. Derrible and Kennedy [14] introduced robustness indicators corresponding to the characteristics of transit systems by looking at 33 metro systems in the world. They provided recommendations for increasing the robustness of different-sized metro networks. De-Los-Santos et al. [15] provided passenger robustness measures for the rail transit network under without-bridging and with-bridging interruptions. They verified the measures on the Madrid commuter system. Cadarso et al. [16] studied the disruption management problem of rapid transit rail networks. They proposed a two-step approach that combined an integrated optimization model for the timetable and rolling stock with a model for the passengers' behavior.

It is worth mentioning that while the concepts of reliability, resilience and robustness are closely related to the general subject of vulnerability [17], these neighboring terms are different in research scopes. Vulnerability in transport is more a characteristic of the system itself, and concerns more about the consequences and probabilities of system failures [18]. Therefore, the above mentioned literatures constitute a tool for addressing vulnerability related problems, but they did not directly look into the issue of vulnerability.

Currently, vulnerability analysis of urban rail transit networks mainly referred to the research achievements in road network systems [19-20]. Gao [21] proposed an evaluating model of metro network invulnerability on the basis of network topology and calculated the evaluating indices with matrix logic. Wang [22] constructed the topological model of Beijing transit network and simulated the network efficiency under attacks. Zhang et al. [23] measured the topological characteristics and functional properties of Shanghai subway network. This research indicated that the subway network was robust against random attacks but fragile to intentional attacks. Ye [24] applied the same methodology to study the topological characteristics of Chongqing rail transit network and evaluated the vulnerabilities of every station under attacks. Nevertheless, these studies simplified the urban rail transit networks with graph theory and therefore, lacked considerations of properties that are characteristic of rail transit systems, such as the ability to transfer, etc.

Several other approaches to the vulnerability analysis were employed by scholars. Quan et al. [25] established an index system to assess the vulnerability of rainstorm water-logging in Shanghai subway. Han et al. [26] analyzed the urban mass transit accident from three aspect, including interference, exposure and vulnerability. They regarded vulnerability as the inherent defects of the system and established a safety insurance mechanism based on this theory. Yuan et al. [27] studied the statistical data of metro network accidents and proposed the concepts of physical, structural and social vulnerabilities of metro system. These studies, however, lacked systematical analysis of urban rail transit networks operation, which may hinder the usefulness to public transportation planners and practitioners.

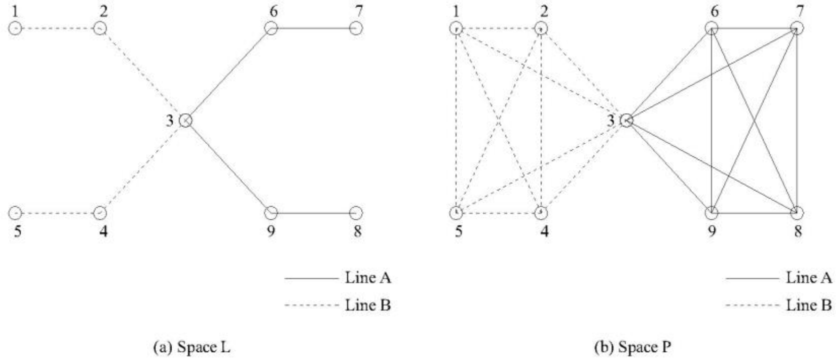
2 Application of Complex Network Theory

2.1 Complex network theory

Complex network is defined as network model whose vertices are the elements of the system and whose edges represent the interactions between them [28]. Many systems could be defined as complex networks, such as Internet and social networks. According to Angeloudis and Fisk' [7] study of 20 world's largest subways, urban rail transit networks could also be depicted as complex networks. They possess the characteristics of high connectivity but low maximum vertex degree, and could be grouped as small-world, scale-free networks.

2.2 Construction of urban rail transit networks

Normally, network topology could be constructed with the following two methods: (1) Space L method, with which vertices are connected only if they are adjacent; (2) Space P method, with which vertices are connected as long as they have direct path to reach each other.



(a) Space L

(b) Space P

Figure2-1 Network Construction Methods

Stations and traffic lines are the basic components in urban rail transit networks. With Space L method, stations could be abstracted into nodes of complex networks while traffic lines could be abstracted into edges that connect nodes. As urban metro is two-way traffic, the rail transit network could be viewed as an undirected graph $\mathrm{G} = \langle V, E \rangle$. In the network, $\mathrm{V} = \{v_i | i = 1,2,3 \dots N\}$ is the set of network nodes, and $\mathrm{E} = \{e_{ij} | v_i, v_j \in V\}$ is the set of network edges. $\mathrm{A} = [a_{ij}]_{n \times n}$ is the network adjacent matrix, in which a_{ij} is defined as:

$$a_{ij} = \begin{cases} 1, (v_i, v_j) \in E \\ 0, (v_i, v_j) \notin E \end{cases} \tag{2.1}$$

Also, as the rail transit network is an undirected graph, we have $e_{ij} \in E \Leftrightarrow e_{ji} \in E$, which means that the network adjacent matrix A is a symmetric non-negative matrix.

2.3 Topological index

Topological parameters are the basic tools to study network characteristics in complex network theory. Therefore, we define and explain here several topological indexes which would be used in our later analysis of network vulnerability. Commonly speaking, main topological parameters of complex networks include degree, average degree, betweenness, average betweenness, shortest path, average shortest path length, topological efficiency, clustering coefficient, etc.

2.3.1 Degree

Degree (D_i) is defined as the number of edges that connected with node v_i. It reveals the connectivity of the node. Therefore, Average Degree (AD) of the network is defined as:

$$\mathrm{AD}=\frac{1}{N}\sum_{i=1}^{N}D_i \tag{2.2}$$

where N is the number of nodes in the network.

2.3.2 Connectivity Factor

Connectivity Factor (CF) is defined as:

$$\mathrm{CF}=\frac{1}{N}\sum_{v_i,v_j\in V}e_{ij} \tag{2.3}$$

It reveals the overall connectivity of the network.

2.3.3 Betweenness

Betweenness (B_i) is defined as the number of times that the shortest paths between any two nodes in the network go through node v_i. The shortest path between two nodes is the minimum number of edges between them. Betweenness reveals the importance of the node in the transmission of information. Therefore, Average Betweenness (AB) of the network is defined as:

$$\mathrm{AB}=\frac{1}{N}\sum_{i=1}^{N}B_i \tag{2.4}$$

2.3.4 The Shortest Path

The Shortest Path (l_{ij}) between two nodes v_i and v_j is the minimum number of edges between them. It depicts the transit efficiency between the two. In another word, the smaller l_{ij} is, the more efficient of information transmission between v_i and v_j would be. Therefore, Average Shortest Paths (ASP) of the network is defined as:

$$\mathrm{ASP}=\frac{1}{N(N-1)}\sum_{v_i,v_j\in V}l_{ij} \tag{2.5}$$

As defined in Equation (2.5), if the network is non-connected, and v_i and v_j belong to different isolated networks, we have $l_{ij}=\infty$ and also $\mathrm{ASP}=\infty$.

2.3.5 Topological Efficiency

When network is non-connected, the shortest path defined above could not be used to depict network transmission efficiency any more. To avoid such problem, Topological Efficiency (E) is proposed and defined as:

$$\mathrm{E}=\frac{1}{N(N-1)}\sum_{v_i,v_j\in V}\frac{1}{l_{ij}} \tag{2.6}$$

It depicts the overall connectivity of the network and at the same time, avoids the problem in Equation (2.5). When the network consists of several non-connected sub-networks, and v_i and v_j belongs to different sub-networks, we have $l_{ij}=\infty$ and also $1/l_{ij}=0$.

2.3.6 Clustering Coefficient

If V_i is the set of adjacent nodes of node v_i, we could define Clustering Coefficient (C_i) of v_i as:

$$C_i=\frac{2|E_i|}{N_i(N_i-1)} \tag{2.7}$$

where $N_i=|V_i|$ is the number of elements in set V_i and $\mathrm{E}_i=\left\{e_{ij}\middle|(v_i,v_j)\in E\wedge v_j\in V_i\right\}$. It depicts the clustering ability of the node. Therefore, Average Clustering Coefficient (AC) of the network is defined as:

$$\mathrm{AC} = \frac{1}{N}\sum_{i=1}^{N} C_i = \frac{1}{N}\sum_{i=1}^{N} \frac{2|E_i|}{N_i(N_i-1)} \tag{2.8}$$

It could reveal the aggregation degree of the network, but it does not represent the overall connectivity of the whole network.

Among the above mentioned indexes, degree depicts network connectivity while betweenness depicts network pressure. The average shortest path between any two nodes in the network depicts network transit efficiency. Topological efficiency is based on the calculation of the shortest path and is the best parameters to depict overall connectivity of network. Clustering coefficient depicts connectivity of node, but it is not accurate to depict the overall connectivity of the network.

3 Network Vulnerability Model

Vulnerability in traffic area is defined as “a susceptibility to incidents that can result in considerable reductions in network serviceability”. [18] It involves two parts generally: (1) the probability that an event would happen and cause negative impacts, and (2) the negative consequences once the event has taken place. In vulnerability studies, negative impact minimization is an important aspect as it is often hard to predict the probabilities of certain events, such as terrorist actions and extreme weathers, etc. Therefore, it is necessary to be expected possible consequences and be prepared.

3.1 Network malfunctions

To better study the vulnerability of urban rail transit networks, we firstly discuss network malfunctions. Network malfunctions could be grouped into two types: internal and external. Internal malfunctions are caused by system errors, such as system aging, internal disturbances, etc. External malfunctions are caused by external factors, such as natural disasters, malicious attacks, etc. There are two types of malicious attacks: node-based and edge-based. In this paper, we mainly study the node-based attacks and group such attacks into three types: the largest degree node-based attacks, the highest betweenness node-based attacks and random attacks.

(1) The largest degree node-based attacks: starting from the initial state, to delete the node with the largest degree in each step and re-calculate the network status. In this way, nodes are deleted one by one.

(2) The highest betweenness node-based attacks: starting from the initial state, to delete the node with the highest betweenness in each step and re-calculate the network status. Similar to Rule (1), nodes are also deleted one by one.

(3) Random attacks: starting from the initial state, to delete a node in the network randomly in each step and re-calculate the network status. Just as in Rule (1) and Rule (2), nodes are deleted one by one.

3.2 Evaluation model

We study the urban rail transit networks from two sides: topological vulnerability and functional vulnerability.

Topological Vulnerability is defined as the network susceptibility to incidents that could result in a reduction in structure connectivity. Several parameters could be applied to depict the overall efficiency and connectivity of the network, such as Connectivity Factor, Topological Efficiency and the Average Shortest Path. Among these parameters, we use Topological Efficiency to evaluate network topological vulnerability.

As defined in Equation (2.6), Topological Efficiency $\mathrm{E} = \frac{1}{N(N-1)} \sum_{v_i, v_j \in V} \frac{1}{l_{ij}}$. It depicts the overall connectivity of the network. With a higher value of E, we could have a more efficient network information transmission.

When node v_i is attacked and removed from the network, the value of E would change as well. Therefore, we define the topological efficiency of v_i [E(v_i)] as:

$$\mathrm{E}(v_i) = \mathrm{E}(\mathrm{O}) - \mathrm{E}(v'_i) \tag{3.1}$$

where E(O) is the original topological efficiency of the network and E(v'$_i$) is the network topological efficiency after v_i being attacked. The higher value of E(v_i) is, the greater impact v_i would have on network efficiency. In another word, v_i is more critical to topological reliability.

Functional Vulnerability is defined as the network susceptibility to incidents that could result in a reduction in transport ability. We suppose that each node in the network possesses the initial functional ability of 1. If a node is removed from the network (attacked or isolated), its functional ability reduced to 0. Based on this definition, we could therefore use network size to evaluate network functional vulnerability.

When network is attacked, the attacked node would be removed from the network. Meanwhile, it would cause some isolated nodes in the network, which would also be deleted. Therefore, we define Network Size as the total number of remaining nodes in the network.

To better analyze network transport ability, we also define and use the concept of Origin-Destination (OD) in urban rail transit networks. When node v_i is attacked, several ODs in the network would become unconnected. Therefore, we define OD Susceptibility of v_i [S(v_i)] as:

$$\mathrm{S}(v_i) = 1 - \frac{|S(v'_i)|}{|S(O)|} \tag{3.2}$$

where |S(O)| is the number of OD in the original network and |S(v'$_i$)| is the number of remaining connected OD after v_i being attacked. It reveals the importance of node v_i in maintaining network functional properties.

Some previous literatures also use Largest Connected Cluster (LCC) [23] to evaluate functional vulnerability of urban rail transit networks. LCC is defined as the network size of the largest sub-network after the network being attacked. However, this parameter is not suitable to evaluate urban rail transit networks as trains could still operate in each sub-network even if the network is attacked and divided into several isolated sub-networks.

4 Vulnerability Analysis of Shanghai Metro

4.1 Basic network information

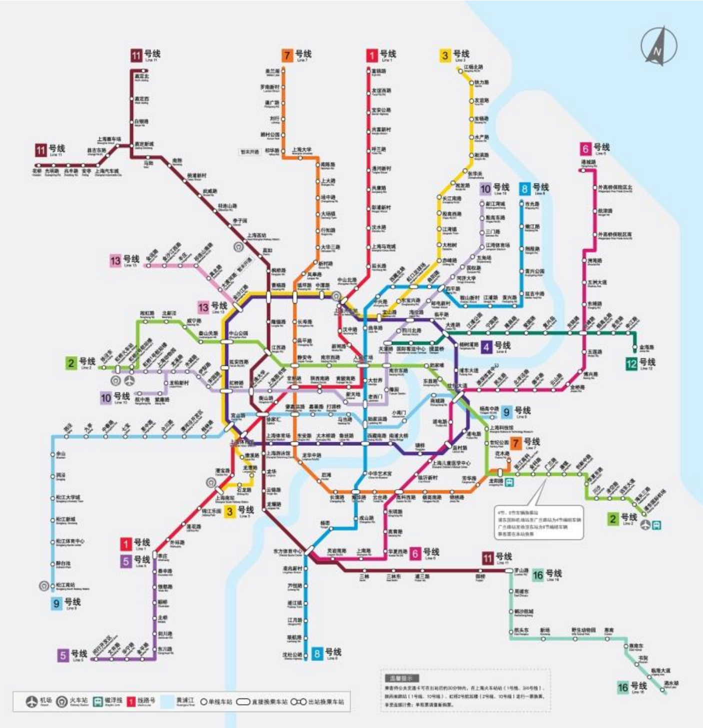


Figure4-1 Shanghai Metro Route Map

In this section, Shanghai Metro is studied based on the above vulnerability model. Figure4-1 presents the route map of Shanghai Metro. As can be seen from the figure, Shanghai Metro is a very complicated transport system with 14 lines (Line1-13 and Line16) in operation. The network topology is constructed and basic parameter information is obtained with C++ and Matlab. Table4-1 presents the summary of Shanghai Metro topological characteristics. Currently, there are 287 nodes and 317 edges in the network. The average degree is 2.2, which is at the average level among urban rail transit networks in major cities around the world. Figure4-2 presents the degree distribution of Shanghai Metro network. The nodes with degree 2 take up approximately 80% of the total number while the nodes with degree 4 take up approximately 9%. There is only 1 node with degree 8 and 2 nodes with degree 6 and 5 respectively, which means that the nodes with large degree are very few in quantities.

Table4-1 Characteristics Index of Shanghai Metro

Characteristics Index	Value
Node No.	287
Edge No.	317

Average Degree	2.2
Connectivity Factor	1.105

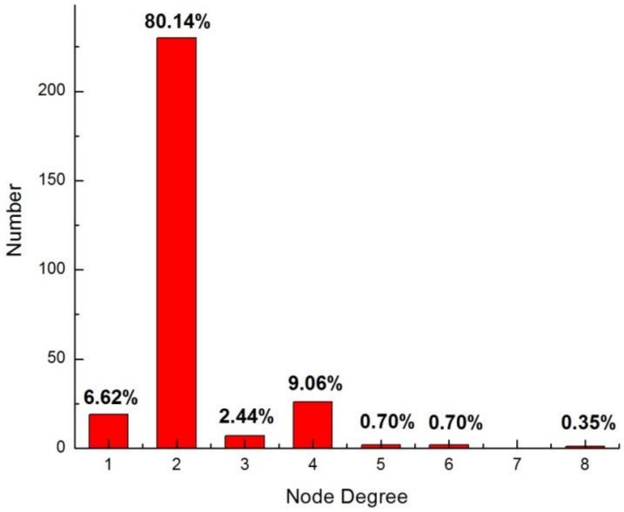


Figure4-2 Degree Distribution of Shanghai Metro

Table4-2 presents the top 10 important stations of Shanghai Metro based on node degree and node betweenness respectively. Century Avenue is the node with the largest degree of 8. It means that the station is connected with other 8 stations in the network. Xujiahui possesses the largest node betweenness of 23624. It means that there are overall 23624 shortest paths in the network go through Xujiahui station. It is also worth noticing that the two rankings are quite different from each other. Some stations, such as Caoyang Road, Zhenping Road and Jiangsu Road, which are of node degree 4, possess higher node betweenness than Century Avenue and People’s Square.

Table4-2 Top10 Important Stations of Shanghai Metro

Station Ranking based on Node Degree			Station Ranking based on Node Betweenness		
No.	D_i	Station	No.	B_i	Station
1	8	Century Avenue	1	23624	Xujiahui
2	6	Xujiahui	2	20104	Caoyang Road
3	6	People's Square	3	18232	Zhenping Road
4	5	Oriental Sports Center	4	17306	Jiangsu Road
5	5	Yishan Road	5	17264	Century Avenue
6	4	South Shaanxi Road	6	17222	Shanghai Railway Station
7	4	Changshu Road	7	16448	Jiaotong University
8	4	Shanghai Railway Station	8	15218	Hailun Road
9	4	Shanghai Indoor Stadium	9	14804	People's Square
10	4	Zhaojiabang Road	10	14120	Baoshan Road

4.2 Topological vulnerability analysis of Shanghai Metro

Figure4-3 depicts the changes in network efficiency of Shanghai Metro under malicious attacks. The original network efficiency is only 0.008. It means that the overall connectivity of the network is poor. As can be seen from the figure, random attacks cause the minimal losses in network efficiency among the three malicious attacks. When 10% of nodes (29 nodes) are attacked and removed from the network, the network efficiency decrease by only 14%. However, both of the largest degree node-based attacks and the highest betweenness node-based attacks cause great losses in network efficiency. When 10% of nodes are deleted from the network, the network efficiencies decrease by 37% and 34% respectively. There is little difference in these two ways of attacks. It means that stations with high node betweenness are of same influence on network efficiency as stations with large node degree. These stations may not be important in common sense, but they have great impact on maintaining network connectivity. This figure also illustrates that urban rail transit networks are vulnerable to the largest degree node-based attacks and the highest betweenness node-based attacks, but it is quite robust to random attacks.

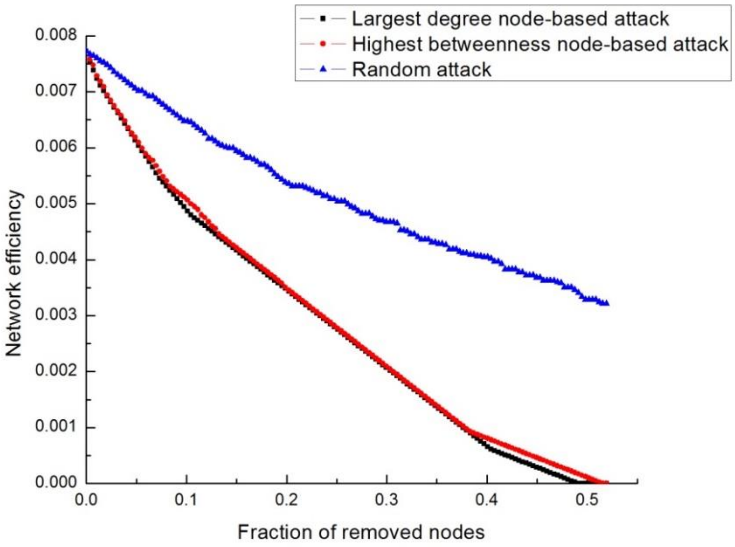


Figure4-3 Network Efficiency of Shanghai Metro under Malicious Attacks

4.3 Functional vulnerability analysis of Shanghai Metro

Figure4-4 depicts the changes in network size of Shanghai Metro under malicious attacks. The largest degree node-based attacks cause the maximum losses in network size among the three malicious attacks. When 20% of nodes (58 nodes) are attacked and removed from the network, the network size decrease by 39%. Apart from the 58 attacked nodes, it also causes 54 isolated nodes in the network. This figure illustrates that the stations with large node degree are important to maintaining network transport ability. These stations are also critical to other stations in the network.

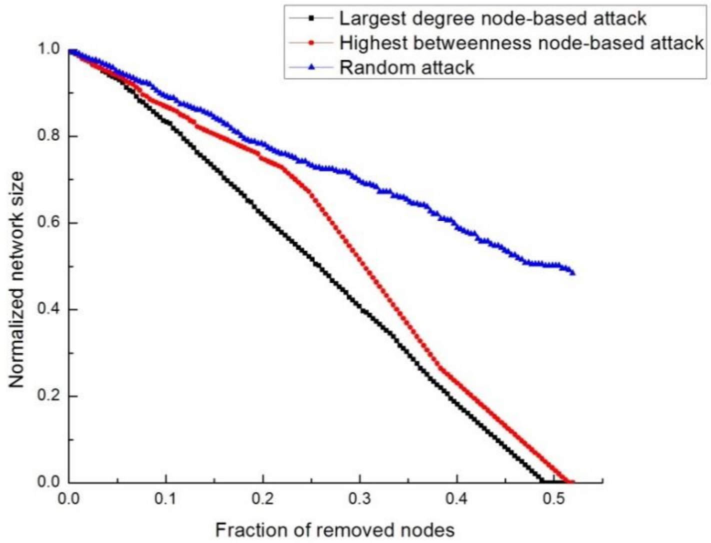


Figure4-4 Network Size of Shanghai Metro under Malicious Attacks

Figure4-5 depicts the changes in connected OD ratio of Shanghai Metro under malicious attacks. As can be seen from the figure, malicious attacks have a great impact on OD connectivity. When the top 7 stations with the highest betweenness are attacked, the connected OD ratio decreases to only 29%. Moreover, when 10% of nodes (29 nodes) are attacked and removed from the network, the connected OD ratio decrease to approximately 2% under both of the largest degree node-based attacks and the highest betweenness node-based attacks. Only 760 OD pairs are still connected out of 41041 original pairs and the network is paralyzed. This figure illustrates that OD connectivity is vulnerable to malicious attacks.

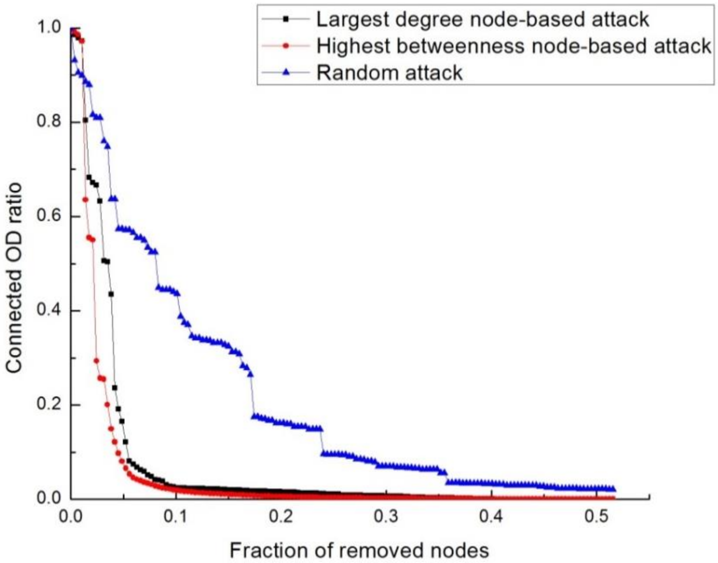


Figure4-5 Connected OD Ratio of Shanghai Metro under Malicious Attacks

5 Comparisons of Different Urban Rail Transit Networks

5.1 Basic network information

To better understand and explore reliable network geometry, we would study and compare the vulnerabilities of different urban rail transit networks, namely Shanghai Metro, Taibei Metro and Tokyo Metro in this section. Figure5-1 and Figure5-2 presents the route map of Taibei Metro and Tokyo Metro respectively. As can be seen from these two figures, Taibei Metro has a simple structure while Tokyo Metro is a super complicated system.

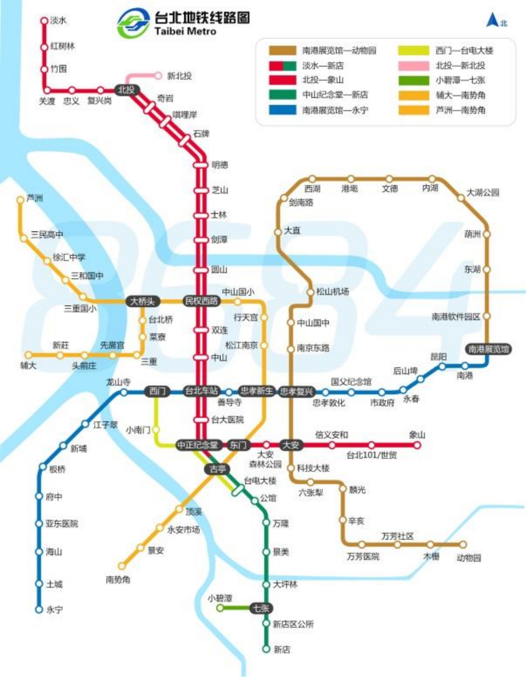


Figure5-1 Taibei Metro Route Map

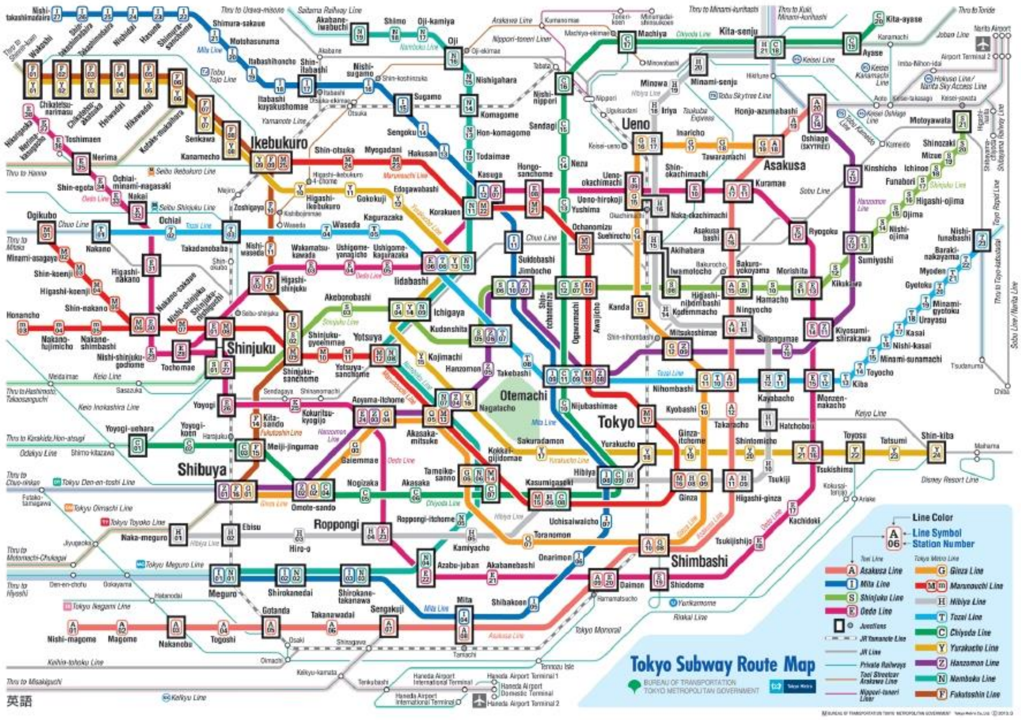


Figure5-2 Tokyo Metro Route Map

Table5-1 presents the comparison of basic topological characteristics of the three metros. Shanghai Metro possesses the maximum number of nodes while Taibei Metro has only 101 nodes in total. However, Tokyo Metro possesses the highest average degree and connectivity factor than the other two. It means that Tokyo Metro enjoys the best overall network connectivity. Figure5-3 presents the degree distributions of the three metros. Different from Shanghai Metro and Taibei Metro, the nodes with degree 2 take up only 70% of the total number in Tokyo Metro. Instead, there are more nodes with large degree in Tokyo Metro with 5 nodes of degree 6 and 10 nodes of degree 5. It reveals the better connectivity of Tokyo Metro.

Table5-1 Characteristics Index of the Three Metros

Characteristics Index	Shanghai	Tokyo	Taibei
Node No.	287	204	101
Edge No.	317	256	105
Average Degree	2.2	2.5	2.1
Connectivity Factor	1.105	1.255	1.040

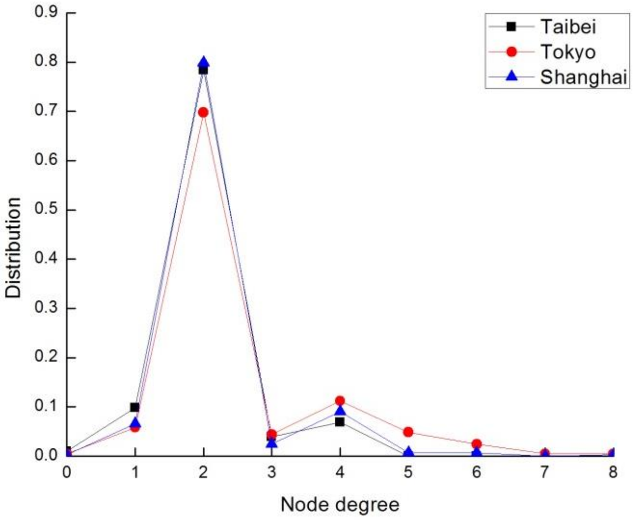


Figure5-3 Degree Distributions of the Three Metros

5.2 Topological vulnerability analysis

Figure5-4, Figure5-5 and Figure5-6 depict the changes in network efficiency of the three metros under malicious attacks. As can be seen from Figure5-4, under the largest degree node-based attacks, when less than 10% of the nodes are attacked and removed from the networks, the changes in network efficiencies are similar to Tokyo Metro and Shanghai Metro. It means that the critical nodes (nodes with large degree) in these two metros possess similar robustness to malicious attacks. However, when 20% of the nodes (57 nodes in Shanghai Metro and 41 nodes in Tokyo Metro) are attacked and removed from the networks, the network efficiencies decrease by 55% and 60% respectively for Shanghai Metro and Tokyo Metro. The attacks in Tokyo metro cause a greater loss in network efficiency. In another word, these less critical nodes (nodes with degree 2 or 3) in Tokyo Metro account for higher network efficiencies than those in Shanghai Metro. It reveals that Tokyo Metro is not only robust for critical-station attacks, but also more economical in constructing other less critical stations. Similar conclusions could be reached from Figure5-5 and Figure5-6 when Tokyo Metro and Shanghai Metro are compared. Taibei Metro is not taken into considerations here as generally speaking, network efficiency is relevant with total node number in the network and makes it hard to compare a simple network (Taibei Metro) with complicated ones (Shanghai Metro and Tokyo Metro).

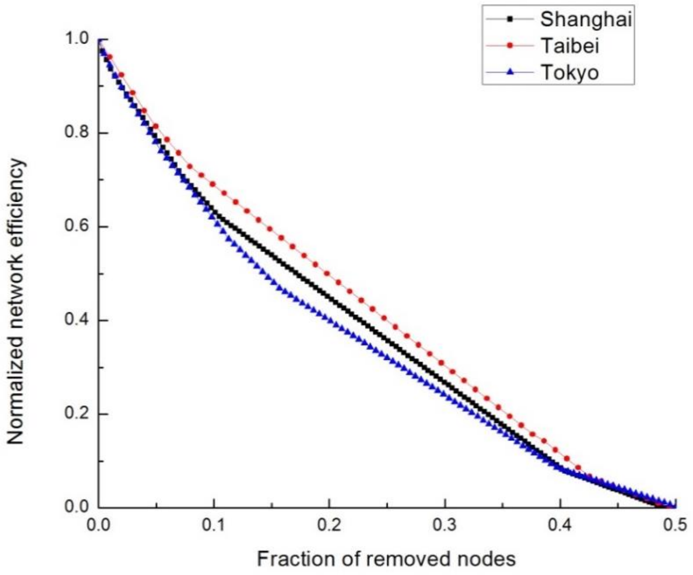


Figure5-4 Network Efficiency under the Largest Degree Node-based Attacks

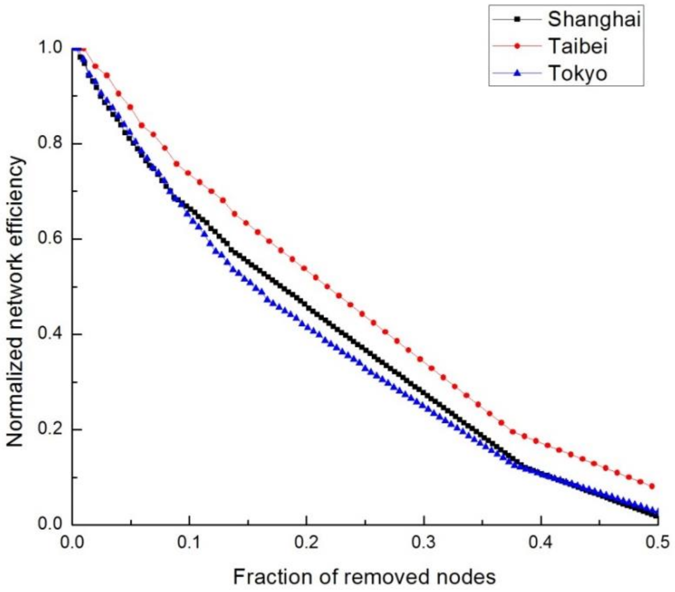


Figure5-5 Network Efficiency under the Highest Betweenness Node-based Attacks

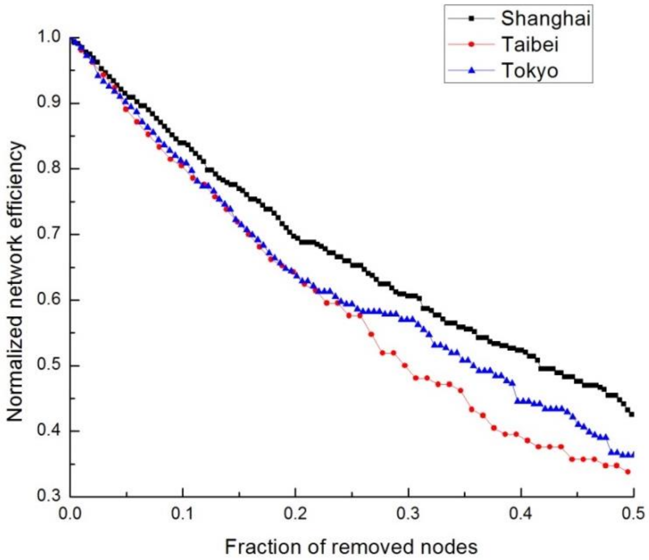


Figure5-6 Network Efficiency under Random Attacks

5.3 Functional vulnerability analysis

Figure5-7, Figure5-8 and Figure5-9 depict the changes in network size of the three metros under malicious attacks. For all the three metros, the largest degree node-based attacks cause the maximum losses in network size among the three malicious attacks. Therefore, we put our emphasis on the study of the largest degree node-based attacks. As can be seen from Figure5-7, when less than 10% of the nodes are attacked and removed from the networks, the changes in network sizes are similar to the three metros. However, when more than 10% of the nodes are attacked, the changes in network size of Tokyo Metro are obviously smaller than the changes in Shanghai Metro and Taibei Metro. It means that the attacks cause fewer ratios of isolated nodes in Tokyo Metro than the other two. In another word, Tokyo Metro possesses the best transport ability under malicious attacks among the three metros.

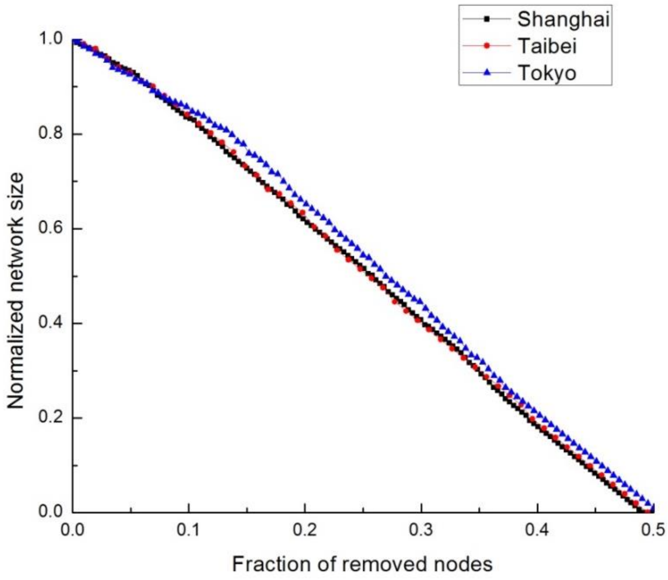


Figure5-7 Network Size under the Largest Degree Node-based Attacks

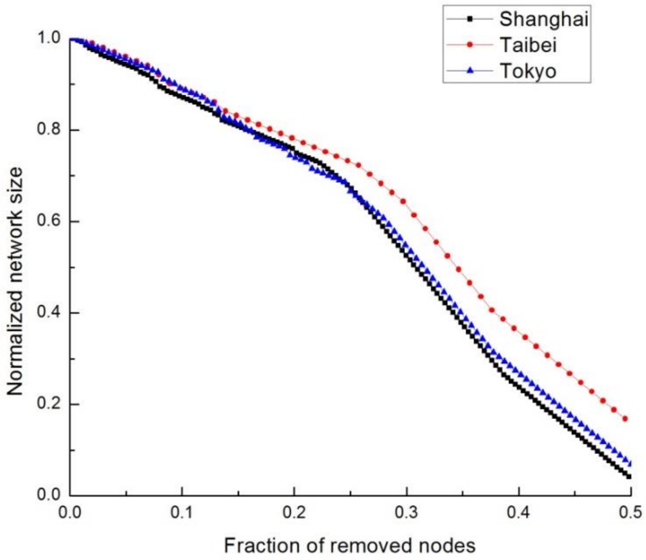


Figure5-8 Network Size under the Highest Betweenness Node-based Attacks

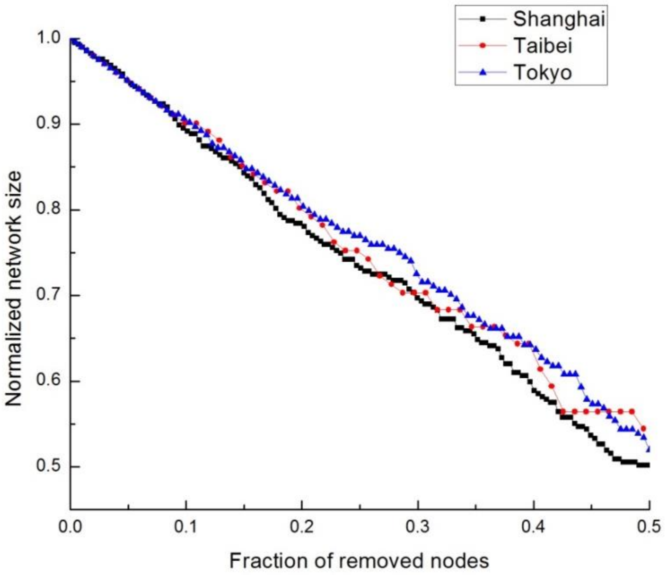


Figure5-9 Network Size under Random Attacks

Figure5-10, Figure5-11 and Figure5-12 depict the changes in connected OD ratio of the three metros under malicious attacks. Different from Shanghai Metro and Taibei Metro, Tokyo Metro is much more robust to the largest degree node-based attacks. When 8% of nodes (16 nodes) are attacked and removed from the network, there are still 45% of OD pairs connected in Tokyo Metro. 9345 OD pairs are connected out of 20706 original pairs. The ratio is much higher than that of Shanghai Metro and Taibei Metro. However, the OD connectivity of Tokyo Metro is as vulnerable as that of Shanghai Metro and Taibei Metro under the highest betweenness node-based attacks. When 8% of nodes (16 nodes) are attacked and removed from the network, the connected OD ratio decrease to only 9% in Tokyo Metro. It reveals that stations with high node betweenness are more critical to OD connectivity than stations with large degree, and therefore need to be protected.

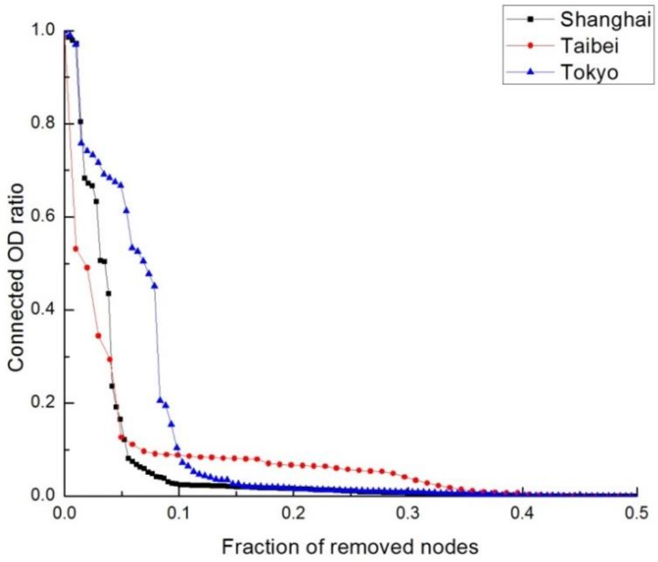


Figure5-10 Connected OD Ratio under the Largest Degree Node-based Attacks

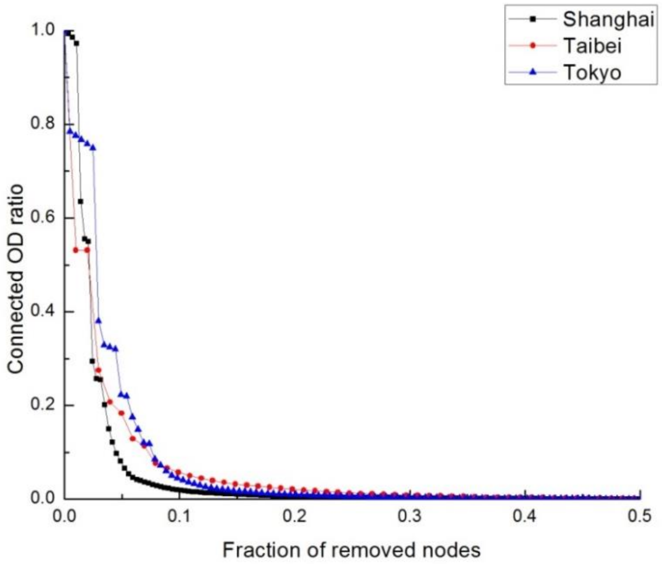


Figure5-11 Connected OD Ratio under the Highest Betweenness Node-based Attacks

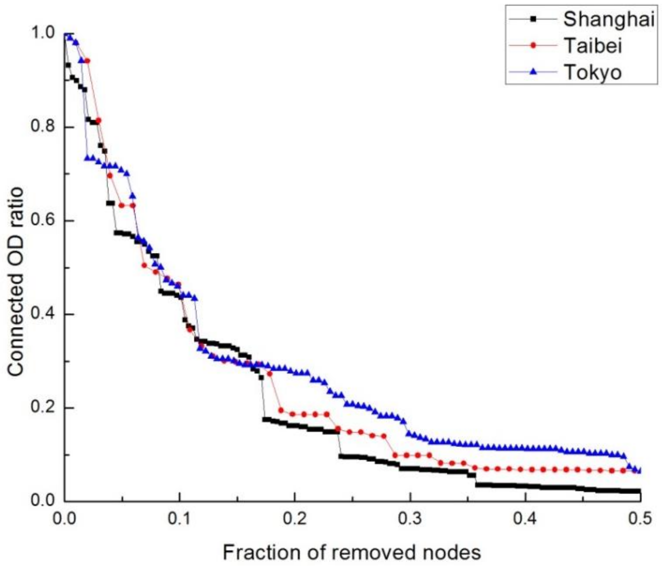


Figure5-12 Connected OD Ratio under Random Attacks

6 Conclusions

Based on the above analysis, we could reach the following conclusions:

(1) Urban rail transit network is quite robust to random attacks, but it is vulnerable to the largest degree node-based attacks and the highest betweenness node-based attacks.

(2) Stations with high node betweenness are of same influence on network efficiency as stations with large node degree. These stations may not be important in common sense, but they have great impact on maintaining network connectivity.

(3) Stations with large node degree are more important to maintaining network size while stations with high node betweenness are more critical to maintaining OD connectivity.

(4) Tokyo Metro is not only robust for critical-station attacks, but also more economical in constructing other less critical stations. It possesses the best transport ability under malicious attacks among the three metros and is much more robust to the largest degree node-based attacks in OD connectivity.

These conclusions can provide both theoretical significance and practical significance to the study of rail transit networks. Critical stations could be identified in the network and be better protected. Tokyo Metro could be taken as a model for the construction of urban rail transit networks around the world. In the meanwhile of guaranteeing network reliability, it also provides ideas on reducing construction costs.

However, there are still some problems existing in current vulnerability model. To traffic users (metro passengers), interchange times is an important factor which would affect their route choices, but the above mentioned evaluation indexes are hard to depict transfer efficiency. In the next step of our research, the time required to transfer as well as the passengers psychological habits would be quantified in the model. As large passenger flow would add pressure to the network system and increase the probability of breakdown, traffic volume would also be quantified in the model.

Reference

[1] Musso A, Vuchic V R. Characteristics of metro networks and methodology for their evaluation[M]. 1988.

[2] 张新军, 赵小琴. 世界城市地铁与轻轨最新动态[M]. 中国铁道出版社, 2001.

[3] Vuchic V R. Urban transit[M]. Wiley, 2005.

[4] Latora V, Marchiori M. Is the Boston subway a small-world network?[J]. Physica A: Statistical Mechanics and its Applications, 2002, 314(1): 109-113.

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

[6] Vragović I, Louis E, Diaz-Guilera A. Efficiency of informational transfer in regular and complex networks[J]. Physical Review E, 2005, 71(3): 036122.

[7] Angeloudis P, Fisk D. Large subway systems as complex networks[J]. Physica A: Statistical

Mechanics and its Applications, 2006, 367: 553-558.

[8] Lee K, Jung W S, Park J S, et al. Statistical analysis of the Metropolitan Seoul Subway System: Network structure and passenger flows[J]. Physica A: Statistical Mechanics and its Applications, 2008, 387(24): 6231-6234.

[9] Raveau S, Muñoz J C, De Grange L. A topological route choice model for metro[J]. Transportation Research Part A: Policy and Practice, 2011, 45(2): 138-147.

[10] 赵惠祥. 城市轨道交通系统的运营安全性与可靠性研究[D]. 同济大学, 2006.

[11] Beroggi G E G. Integrated safety planning for underground systems[J]. Journal of hazardous materials, 2000, 71(1): 17-34.

[12] Canós J H, De Zulueta F. Using hypermedia to improve safety in underground metropolitan transportation[J]. Multimedia Tools and Applications, 2004, 22(1): 75-87.

[13] 徐瑞华, 张铭, 王志强. 基于工作流的轨道交通应急管理系统设计与实现[J]. 同济大学学报: 自然科学版, 2008, 36(6): 754-759.

[14] Santiago del Río P M, Hernández J A, Aracil J, et al. A reliability analysis of Double-Ring topologies with Dual Attachment using p-cycles for optical metro networks[J]. Computer Networks, 2010, 54(8): 1328-1341.

[15] Derrible S, Kennedy C. The complexity and robustness of metro networks[J]. Physica A: Statistical Mechanics and its Applications, 2010, 389(17): 3678-3691.

[16] De-Los-Santos A, Laporte G, Mesa J A, et al. Evaluating passenger robustness in a rail transit network[J]. Transportation Research Part C: Emerging Technologies, 2012, 20(1): 34-46.

[17] Cadarso L, Marín Á, Marótì G. Recovery of disruptions in rapid transit networks[J]. Transportation Research Part E: Logistics and Transportation Review, 2013, 53: 15-33.

[18] Berdica K. An introduction to road vulnerability: what has been done, is done and should be done[J]. Transport Policy, 2002, 9(2): 117-127.

[19] Jenelius E, Petersen T, Mattsson L G. Importance and exposure in road network vulnerability analysis[J]. Transportation Research Part A: Policy and Practice, 2006, 40(7): 537-560.

[20] Bell M G H, Kanturska U, Schmöcker J D, et al. Attacker–defender models and road network vulnerability[J]. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 2008, 366(1872): 1893-1906.

[21] 高洁, 施其洲. 城市轨道网络抗毁可靠性定义及评价指标模型研究[J]. 铁道学报, 2007, 29(3): 29-29.

[22] 王云琴. 基于复杂网络理论的城市轨道交通网络连通可靠性研究[D]. 北京: 北京交通大学, 2008.

[23] Zhang J, Xu X, Hong L, et al. Networked analysis of the Shanghai subway network, in China[J]. Physica A: Statistical Mechanics and its Applications, 2011, 390(23): 4562-4570.

[24] 叶青. 基于复杂网络理论的轨道交通网络脆弱性分析[J]. 中国安全科学学报, 2012, 22(2): 122-126.

[25] 权瑞松, 刘敏, 张丽佳. 上海市地下轨道交通暴雨内涝脆弱性评价[J]. 人民长江, 2011, 42(15): 13-17.

[26] 韩豫, 成虎, 赵宪博, 等. 基于脆弱性的城市轨道交通运营安全理论框架[J]. 城市轨道交通研究, 2012, 15(11): 15-19.

[27] 袁竞峰, 李启明, 贾若愚, 等. 城市地铁网络系统运行脆弱性分析[J]. 中国安全科学学报, 2012, 22(5): 92-98.

[28] Barabási A L, Albert R. Emergence of scaling in random networks[J]. science, 1999,

286(5439): 509-512.