Public Transp (2017) 9:501–525
DOI 10.1007/s12469-017-0170-2

CASE STUDY AND APPLICATION

Vulnerability analysis of urban rail transit based on complex network theory: a case study of Shanghai Metro

Yingying Xing[1] · Jian Lu[2] · Shengdi Chen[3] · Sunanda Dissanayake[4]

Accepted: 12 August 2017 / Published online: 11 September 2017

Abstract With increasing passenger flows and construction scale, metro systems in metropolises have entered a new era of networking operation and become the most effective way to alleviate and decrease traffic congestion. However, frequent occurrence of random failures and malicious attacks pose a serious threat to metro security and reliability. Thus, it is necessary to quantitatively evaluate the vulnerability of the metro network to different failures or attacks from a networking perspective. Based on the complex network theory, this study took the Shanghai Metro Network (SMN) as an example to investigate vulnerability of a weighted metro network in responding to random failures as well as malicious attacks. In particular, compared to topological networks, the vulnerability of weighted networks was analyzed to investigate how traffic and spatial constraints influence the transport system's vulnerability, since topological features of complex networks are

✉ Jian Lu
jianjohnlu@tongji.edu.cn

Yingying Xing
yingying199004@163.com

Shengdi Chen
sdchen@shmtu.edu.cn

Sunanda Dissanayake
sunanda@ksu.edu

[1] School of Naval Architecture, Ocean and Civil Engineering, Shanghai Jiao Tong University, 800 Dongchuan Road, Shanghai, People's Republic of China

[2] College of Transportation Engineering, Tongji University, 4800 Cao'an Road, Shanghai, People's Republic of China

[3] College of Transport and Communication, Shanghai Maritime University, 1550 Haigang Ave, Shanghai, People's Republic of China

[4] Department of Civil Engineering, Kansas State University, 2118 Fiedler Hall, Manhattan, Kansas 66506, USA

often associated with the weights of the edges and spatial constraints. Simulation results show that the SMN is robust against random failures but fragile for malicious attacks. The vulnerability analysis of weighted properties shows that all targeted attacks are capable to shatter the network's communication or transport properties at a very low level of removed nodes and the highest betweenness attack strategy is the most effective mode to cause destructive effects on SMN among five attack or failure strategies. The inclusion of passenger flows provides evidence for the view that topological networks cannot convey all the information of a real-world network and traffic flow in the network should be considered as one of the key features in the finding and development of defensive strategies. Our results provide a richer view on complex weighted networks in real-world and possibilities of risk analysis and policy decisions for the metro operation department.

Keywords Metro safety · Vulnerability analysis · Complex network · Passenger flow · Robustness

1 Introduction

Due to the increasing traffic volume and growing demands for land because of urban construction and development, many metropolises have continually increased investments in construction of metro lines to relieve serious traffic congestion. With more and more new lines being added into service, many metro systems such as New York City Subway, Shanghai Metro, and Tokyo Metro have transformed into complex metro networks that possess high station densities and intricate inter-station coupling relationships leading to a new era of networking operations (Angeloudis and Fisk 2006; Xu and Sui 2007; Yang et al. 2015). However, recent history has shown that metro systems entail dangerous environments in case of emergencies due to the comparatively enclosed structure and large passenger flows in metro systems. Malicious attacks such as targeted destructions and retaliatory disruptions to the metro system have occurred frequently in recent years; such incidents could result in the functionality loss of the entire system and cause considerable casualties and socio-economic loss. For example, the terrorist attacks that happened in the Lubyanka metro station and Park Kultury metro station of Russia in 2010 killed at least 40 people. In addition, the frequent occurrence of random failures shows that unreasonable planning as well as inadequate safety precautions would impair the overall reliability of a metro system (Albert and Barabási 2002; Newman et al. 2001; Wang 2013; Zhou et al. 2014). It is apparent that increasing size and complexities are making metro systems more dependent on systematic vulnerability analysis and formulation of corresponding coping strategies to increase the robustness of metro networks. However, transit planners pay more attention on traditional characteristics, such as geography, demand, cost and others; none seems to address the network design in a direct way, which becomes increasingly important as transit systems grow. Similarly, transit policymakers and operators considered more about station local properties (such as passenger flows, the number of connected stations) rather than its position and role in the whole metro network. Therefore, it is necessary to conduct a comprehensive analysis of the vulnerability of metro networks from a holistic perspective.

During the past few years, graph and complex network theories have been used to study large-scale transportation infrastructures (railways, highways and airlines) and have become a powerful tool to identify the vulnerable (weak) components (e.g., links or nodes) in a transport network from a systematic view (Ouyang et al. 2014; Taylor et al. 2007; Berdica and Mattsson 2007; Guimerá and Amaral 2004; Wang et al. 2011). By examining public transportation networks of fourteen major cities in the world, Berche et al. (2009) identified public transport network structures which are especially vulnerable and others, which are particularly resilient against attacks. Derrible and Kennedy (2010) analyzed the complexity and robustness of 33 metro systems and provided insights/recommendations for increasing the robustness of metro networks. Laporte et al. (2010) presented an integer linear programming model to design public transit networks in the presence of a link failure and a competing mode. Zhang et al. (2011) investigated the connectivity, robustness and reliability of the subway network by graph theory and complex network theory. According to the analysis and discussion, the study found that the subway network is robust against random attacks but fragile for malicious attacks. Han et al. (2012) analyzed urban mass transit accidents from three aspects, including interference, exposure and vulnerability. They regarded vulnerability as inherent defects of the system and established a theoretical safety insurance mechanism. Yuan et al. (2012) reviewed the statistics of metro accidents and proposed the concepts of physical, structural and social vulnerabilities of metro network systems. Nevertheless, these studies simplified the metro networks with graph theory and considered only the network topology. Thus, they were lacking consideration on dynamic properties of metro systems.

Other approaches to vulnerability analysis of metro networks were also employed. Cats and Jenelius (2012) proposed a dynamic and stochastic notion of public transport network vulnerability and developed a more refined model to assess public transport network vulnerability by considering supply and demand interactions. De-Los-Santos et al. (2012) provided rail transit network robustness measures from the user's point of view. Based on the work of predecessors, Perea and Puerto (2013) discussed and extended a game-theoretic framework for the robust railway network design against intentional attacks. Rodríguez-Núñez and García-Palomares (2014) presented a methodology for analyzing the criticality and vulnerability of a public transport network. Based on the experience of the 7/7 London bombings and other subway incidents, Bruyelle et al. (2014) identified critical systems of metro coach and proposed enhancements to the robustness of subway systems. Taking the Beijing Subway system as an example, Yang et al. (2015) assessed the robustness of a subway network in face of random failures as well as malicious attacks. The research results revealed that the Beijing Subway system exhibits typical characteristics of a scale-free network, with relatively high survivability and robustness when faced with random failures, whereas error tolerance is relatively low when the hubs undergo malicious attacks. Cats et al. (2015) presented and applied a method to explicitly account for exposure in identifying and evaluating link criticality in public transport networks. Chopra et al. (2016) presented a comprehensive, multi-pronged framework that analyzed information on network topology, spatial organization and passenger flow to understand the resilience of the London metro system. Although these studies provide useful insights on network properties that effect reliability and vulnerability of metro systems, an incorporation of passenger flow and geographical space would further enhance network models and provide a richer view on vulnerability analysis of urban rail transit networks. Simulating different station failure situations (single node-multiple nodes-network) under different attack strategies could help to identify critical nodes in the network, which was particularly useful for the rail transit planners and managers.

Therefore, this paper conducts a systematic vulnerability analysis of urban rail transit to provide theoretical support to the planning and operation of urban rail transit networks. The paper focuses on a weighted metro network with traffic and geographical space to explore how traffic and spatial constraints influence the transport system's vulnerability. Different attack strategies including malicious attacks and random failures are discussed to identify the most effective mode to destroy the whole metro network. In particular, the topological, dynamic and damage-depending measures that can be used to identify the most crucial nodes in a weighted network are discussed and compared. The functionality of the whole network depends on the protection of these crucial nodes. Moreover, the vulnerability of weighted networks was analyzed compared to topological networks. According to the findings in this study, several measures are proposed to strengthen the structural robustness of a metro network, which may help in the development of adaptive reactions aimed at dealing with targeted attacks.

2 Background

2.1 Shanghai Metro System

Shanghai is one of the largest cities in China, with more than 20 million people. With a rapidly increasing population, urban traffic congestion in Shanghai becomes even worse which needs to be solved immediately. In order to enhance capacity and accessibility of public transportation, a massive network by a considerable amount over 500 km is constructed and the traffic congestion of ground transportation has been reduced. Until December, 2014, the Shanghai Metro Network (SMN) was the world's largest rapid transit system by route length (Riedel 2014), with 14 lines, 286 stations, 39 transfer stations and a mileage totaling more than 540 km (Fig. 1). It also ranks second in the world by annual ridership after Beijing, with 2.8 billion rides delivered in 2014. The newest daily ridership record was set at 10.286 million on December 31, 2014, while over 8 million people use the system on an average weekday.

The SMN consists of 286 nodes denoting stations and 317 edges accounting for a link connecting two stations which are adjacent to each other. As already observed in previous literatures (Zhang et al. 2011), the topology of the network exhibits both scale-free and small-world properties. Datasets that are provided by the Shanghai

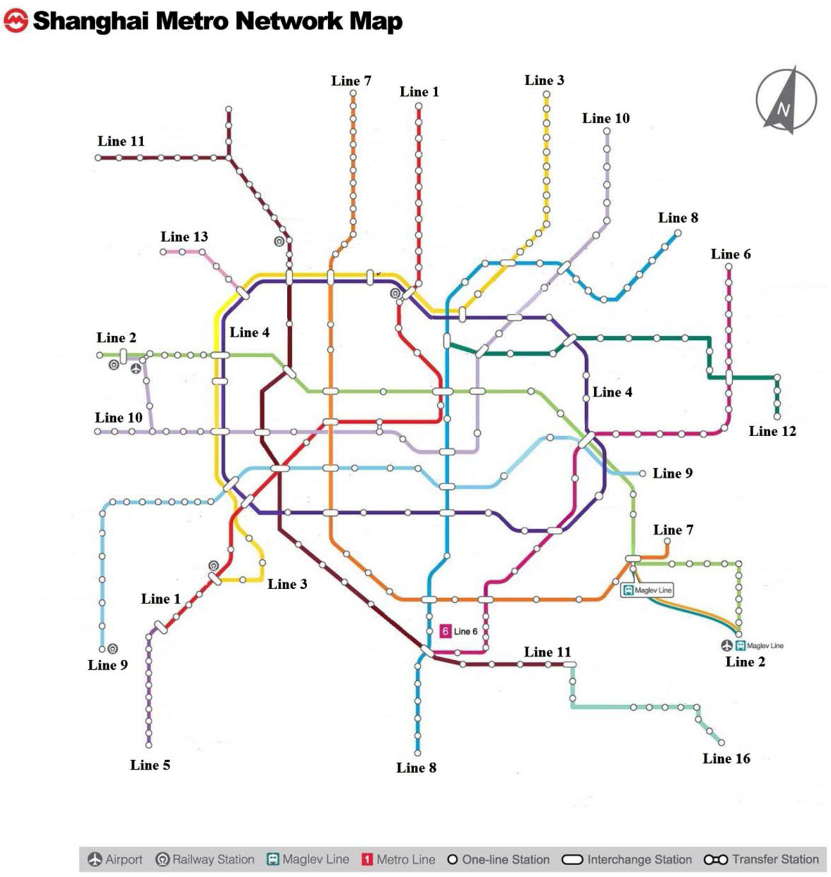


Fig. 1 Schematic map of Shanghai Metro Network (Source: The website of Shanghai Shentong Metro Company)

Shentong Metro Company, list the hourly in and out passenger flows for each station and passenger flows between adjacent stations. In this study, passenger flows during morning peak hours from 7:00 to 9:00 in a typical weekday are analyzed, during which time the highest volume on a weekday could be observed.

2.2 Fundamental concepts of network vulnerability

There is no commonly accepted definition of transport system vulnerability (Mattsson and Jenelius 2015). The definition suggested by Berdica (2002) is often cited by other literatures: "vulnerability in the road transportation system is a susceptibility to incidents that can result in considerable reductions in road network serviceability." This definition can also apply to other modes of transport. Luathep et al. (2011) deem that vulnerability analysis principally focuses on identifying the critical components of the network that result in the most adverse effect on network performance when they are subjected to random failures or malicious attacks. Berdica and Mattsson (2007) propose that vulnerability in transport networks can be seen as overall framework through which different transport studies could be conducted to determine how well a transport system would perform when exposed to different kinds and intensities of disturbances. Berche et al. (2009) note that vulnerability is essential to assess the fault tolerance of a local station as well as a global network. The notion of attack vulnerability is defined as the survivability of a metro network under intentional attacks by Yang et al. (2015). In this study, the concept of network vulnerability is used to describe a lack of serviceability of a metro network when subjected to various threats and hazards. Threats and hazards are the sources of potential damage for a metro network. Hazards refer to accidental events (such as natural disasters and system failures), while threats are related to intentional events (for example, terrorist attacks).

2.3 The definition of various failures

A metro network system generally encounters various emergencies and complex external environments, such as natural disasters, system failures and terrorist attacks, and can be categorized into two types of incidents, i.e., random failures and intentional attacks (Kyriakidis et al. 2012; Wang et al. 2014; Wang 2013). A metro accident is most often due to several different precursors, varying from a natural error to a malicious attack (Kyriakidis et al. 2014; Wang and Fang 2014). Due to the uncertainties of these precursors, it is extremely difficult to quantitatively specify the corresponding destructive power for each failure or attack. As a consequence, an intentional attack in this paper is defined as a malicious or targeted destruction manipulated by artificial forces, while a random failure is specified as the disfunction of a network caused by failure on one or several nodes with a random probability (Ghedini and Ribeiro 2011; Zhang et al. 2012). According to the definition, the main difference between these two incidents is that the probability of a random failure is equal among all stations while an intentional attack generally happens to hub stations with high degree or betweenness centrality. Different precursors of these two incidents are summarized in Table 1.

3 Methodology

3.1 Construction of the weighted SMN model

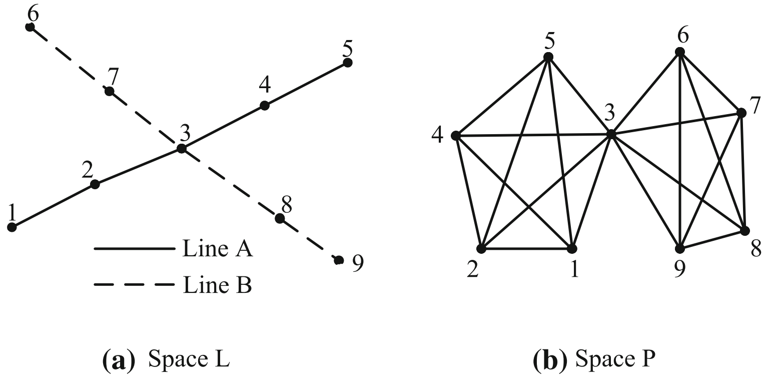
To analyze various properties of urban rail transit systems one should define a proper network topology to describe the structure of the SMN network. Metro systems have been simplified as graphs by using various network representations in previous literature, such as space L, space P, space B, and space C network topologies (Sienkiewicz and Hołyst 2005; von Ferber et al. 2007; Xu et al. 2007a, b; Berche et al. 2010). Each network topology supplies its unique topological insights with respect to metro systems. For instance, space L is mainly applied to investigate topological properties and vulnerabilities of metro systems while space P is widely

Table 1 Summary of common behaviors of failures and attacks for a metro system

Network failure	Precursors categories	Examples
Random failure	Technical failures	Cracked rail/other serious rail defect, broken wheels, loss of brake function, Signal failures, power failure, train doors failure
	Human performance—passenger and metro workers	Congestion, suicide, fall onto track, falls on escalators, fall on stairs, people hit by train, unconscious destruction due to drunkenness, smoke in station/train, passenger carrying dangerous or flammable goods, caught in train doors, wrong operation by driver, exceeding speed limits, signals passed at danger (SPADs)
	Management actions	Station totally closed, Station access closed, Temporary line maintenance
	External environment	Severe weathers, object on track, object exceeding clearance limit
Intentional attack	Malicious or targeted destruction	Terrorism, act of vandalism, passenger carrying dangerous or flammable goods, trespass, set fires, gun shooting, group fighting

used to explore transfer properties like the role of the metro line on transfer times (von Ferber et al. 2007).

As shown in Fig. 2, space L network topology consists of nodes representing stations and edges connecting physically adjacent stations, in other words, an edge between two nodes exists if there is at least one line that provides service to two consecutive stations. No multiple links are allowed (Berche et al. 2009). The node degree k in this topology is just the number of edges that a node shares with others while the distance l is the minimum number of links traversed from one node to another. Space L topology is an intuitive geographical representation of the metro system, and allows us to simulate link failures and analyze their consequences in the



(a) Space L **(b)** Space P

Fig. 2 Explanation of the space L (**a**) and the space P (**b**)

most simplistic manner (Chopra et al. 2016). In the space P, although nodes are the same as in the space L, here an edge between two nodes means that there is at least a direct metro line connecting them. Consequently, the node degree k in this topology is the total number of nodes reachable using a single line and the distance can be interpreted as “the minimum number of line changes $+1$” to be made by a trip maker in order to successfully get from one station to another. This main characteristic allows us to specifically discuss transfer properties of the metro network. Consequently, the Space L representation of the SMN was chosen for our analysis.

Up to now, most studies have focused on unweighted networks, i.e. networks that have a binary nature, where the edges between nodes are either present or not. Nevertheless, along with a complex topological structure, many real networks display a large heterogeneity in the capacity and the intensity of the connections. Therefore, the weighted network was introduced to describe the characteristics and properties of real networks. A weighted graph $G^w = (V, E, W)$, where each edge carries a numerical value measuring the strength of the connection, consists of a set $V = \{v_i | i = 1, 2, \ldots, N\}$ of nodes, a set $E = \{e_{ij} = (v_i, v_j) | i, j = 1, 2, \ldots, N, i \neq j\}$ of edges and a set of weights $W = \{w_{ij} | i, j = 1, 2, \ldots, N, i \neq j\}$ that are real numbers attached to the edges. In matricial representation, G^w could usually be represented by the so-called adjacency weights matrix A^w with adjacency element a_{ij} being defined as

$$a_{ij} = \begin{cases} w_{ij}, & (v_i, v_j) \in E \\ 0 \; or \; \infty, & (v_i, v_j) \notin E \end{cases}, \tag{1}$$

where w_{ij} is the weight of the edge connecting node v_i to node v_j, and $a_{ij} = 0$ or ∞ depends on whether the weight of the edge is dissimilar or similar. The dissimilar weight means that the higher the weight is, the larger the path length and the more aloof the connection between two nodes, for example, the distance in a postman problem. Conversely, the higher the weight is, the smaller the path length and the more intimate the connection between two nodes, the more similar the weight of, for instance, cooperation frequencies in scientific collaboration networks. Therefore, for similar weights, if nodes i and j are connected by node k, the distance $d_{ij} = w_{ik} + \mathrm{w_{kj}}$. For dissimilar weights, the distance is inversely proportional to the edge weight, thus $d^s_{ik} = \frac{1}{w_{ik}}$ and the distance between nodes i and j could be calculated by the equation $d^s_{ij} = \frac{w_{ik} \times w_{kj}}{w_{ik} + w_{kj}}$. Subsequently, based on complex network theory, the stations of the SMN can be represented by the nodes of the network and the lines directly connecting two stations can be virtualized into the edges of the network. Many different quantities of the SMN could be considered as weight of the network, including passenger flow, station spacing, travel time and so on. Moreover, it is assumed that typical travel is bi-directional, and hence the weight w_{ij} of one edge between a pair of nodes (stations) i and j is defined to be the sum of passenger flows in both directions and $w_{ij} = w_{ji}$.

3.1.1 Node degree and strength

The most prominent feature of weighted complex networks is heterogeneity of weights w_{ij} between pairs of nodes, which depicts the interactions between the components in the system. For a given node i in an unweighted network, its degree, $k_i = \sum_j^N a_{ij}$, is the number of nodes it is linked to. Subsequently, in a weighted network, a more meaningful measure of the network properties in terms of the actual weights is obtained by introducing strength s_i, defined as

$$s_i = \sum\nolimits_{j=1}^{N} a_{ij} w_{ij}. \tag{2}$$

From Eq. 2, the quantity s_i combines node degree k_i with edge weight w_{ij}, and is a natural measure of the centrality or connectivity of a node i in the weighted network. For the SMN, the node strength simply accounts for the total passenger flows handled by each station.

3.1.2 Weighted shortest paths

Shortest paths play an important role in the transport and communication within a network. All the shortest path lengths of a graph G can be expressed as a matrix D in which the element l_{ij} is defined as the minimum number of links traversed to get from node v_i to node v_j. Characteristic path length, also known as average path length, is defined as the average number of steps along the shortest paths for all possible pairs of network nodes (Nawrath 2006) and can be expressed by

$$\mathrm{L} = \frac{1}{N(N-1)} \sum\nolimits_{i,j \in V(i \neq j)} l_{ij}. \tag{3}$$

In a generic weighted network, the path length between two nodes v_i and v_j can be introduced as the function of weight w_{ij}, depending on whether the weight of the edge be dissimilar or similar. In this study, the shortest path with the minimum number of edges is not an optimal one. It then defines the weighted shortest path length d_{ij} as the minimum value of the sum of edge lengths throughout all the possible paths from node v_i to node v_j, where the edge length refers to station spacing. It is obvious that the station spacing is a dissimilar weight. Subsequently, the average shortest path length can be defined as

$$\mathrm{L} = \frac{1}{N(N-1)} \sum\nolimits_{i,j \in V(i \neq j)} d_{ij}. \tag{4}$$

3.1.3 Node betweenness

The communication of two non-adjacent nodes depends on the paths connecting them. Consequently, a measure to investigate relevance of a given node can be obtained by counting the fraction of shortest paths between pairs of nodes passing through it, and defining the so-called node betweenness. Together with the degree, the betweenness is one of the standard measures of node centrality and quantifies the influence and importance of a node in the network. More precisely, the betweenness b_i of a node i is defined as (Boccaletti et al. 2006):

$$b_i = \sum\nolimits_{j.k \in V, j \neq k} \frac{n_{jk}(i)}{n_{jk}}, \tag{5}$$

where n_{jk} is the total number of shortest paths from j to k, and $n_{jk}(i)$ is the number of these shortest paths that pass through the node i.

In weighted networks, unequal link capacities make some specific paths more favorable than others in connecting two nodes of the network (Dall'Asta et al. 2006). Thus, it seems natural to generalize the notion of betweenness centrality through replacing shortest paths between pairs of nodes with their weighted versions. Similar to Eq. (5), the weighted betweenness b_i of a node i can be defined as:

$$b_i^w = \sum\nolimits_{j.k \in V, j \neq k} \frac{n_{jk}^w(i)}{n_{jk}^w}, \tag{6}$$

where n_{jk}^w is the total number of weighted shortest paths from j to k, and $n_{jk}^w(i)$ is the number of them that pass through the node i. In the particular case of $w_{ij} = 1$ for all edges, the weighted shortest path length d_{ij} reduces to the minimum number of edges necessary to go from node v_i to node v_j. For metro systems, node betweenness represents status and influence of a station within the network, and central stations are part of more shortest paths than peripheral stations.

3.2 Attack strategies and random failure

An attacking strategy describes the way that an adversary attacks a network, while a random failure is specified as the disfunction of a network caused by accidental incidents. In case of a random failure each node or edge fails with an equal probability. On the contrary, in a malicious attack, an adversary preferentially attacks the target that he believes will maximize the destructive effect on network integrity and functionality. A complex network generally encounters two types of incidents, node attack and edge attack. Considering characteristics of metro systems, a node attack strategy is adopted, that is, attacking a network by removing a node as well as its incident edges from the network. For metro systems, a node removal means that the station is broken down completely and cannot restore function in the short term. Therefore, passengers in the station and travelling on its incident edges cannot reach their destination. Moreover, it is assumed that the purpose of adversaries is to maximize the destructive effect and destroy the network as soon as possible. For this purpose, adversaries first need to evaluate the importance of a node for identifying the most important nodes in the metro network. As a consequence, the ranking mechanism of node importance is crucial for generating an attacking strategy. In general, different adversaries sort the node importance from different aspects, and resulting in different destructive effects.

Based on the different definitions for the centrality ranking of the most important nodes, five different deletion strategies are introduced to investigate the vulnerability of the metro network when subjected to malicious attacks or random failures. Moreover, node centrality measures will be recalculated after each attack. This has been shown to be the most effective strategy (Petter et al. 2002; Dall'Asta et al. 2006), as each node deletion will give rise to a change in the centrality properties of the other nodes. More precisely, the malicious attack strategies and random failures are designed as follows. (1) The malicious attacks according to nodes rank in terms of degree, strength, topological betweenness, and weighted betweenness. That is, from the initial state, the most important node and its incident edges will be deleted and all the properties of weighted networks can be recalculated after a deletion, and the attacks continue. (2) Random failures. The nodes are deleted randomly and the properties of weighted networks can be recalculated after each attack. The nodes will be removed from the network one by one, subjected to these five different attack or failure strategies.

3.3 Assessment model for overall performance of a network

When investigating the assessment model, another key issue to consider is how the global performance of a network under various attacks is measured. Network vulnerability can be characterized in many ways, such as by observing the change of relative size of maximal connected subgraph while nodes are continuously attacked one by one (Crucitti et al. 2003; Berche et al. 2009; Ghedini and Ribeiro 2011). A fast decrease of the largest component size indicates that a network is highly vulnerable. The network performance can also be evaluated by the network efficiency, which is performed by computing possible shortest distance between any two nodes and represents the communication functionality of the network (Zhang et al. 2011; Yang et al. 2015). Therefore, these two indexes were combined to explore how the performance of the SMN responded to different accidents.

3.3.1 Relative size of the largest connected sub-graph

If any two nodes in a graph are connected, the graph G is called a connected graph. When nodes are under attack and deleted from the network, the entire connected graph will disintegrate into multiple subgraphs and disconnected parts (Fig. 3). The largest connected subgraph is the one that has most connected nodes. In the unweighted networks, the largest connected cluster LCC is defined by the relative size of the maximal connected subgraph and can be described as follows

$$LCC = N/N_0, \tag{7}$$

where N is the number of nodes on the largest connected subgraph after attacks, and N_0 is the number of nodes on the largest connected graph of the initial network. In order to assess the reliability and robustness of the weighted networks, the strength s is integrated with the largest connected cluster for the weighted case and LCC^w is defined by the equation

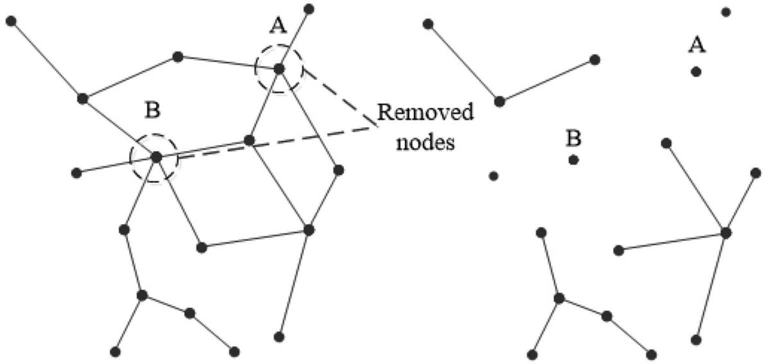


Fig. 3 Structures of the connected graph before and after node removal

$$LCC^w = S/S_0, \tag{8}$$

where S is the sum of the strength of nodes on the largest connected subgraph after attacks, and S_0 is the sum of the strength of nodes on the largest connected graph of the initial network. This quantity measures the structural integrity of the network in reference to strength in local scope, as it refers to the relative traffic or passenger flow that is still handled in the maximal connected component of the network.

3.3.2 Network efficiency

The characteristic path length is a natural measure of the efficiency of a network, and has large implications for the transport and communication in a network. However, when a network is attacked and nodes become disconnected, the shortest path length will be infinite for two unconnected nodes stored in an adjacent matrix and cannot be computed. To overcome this problem, an alternative approach, the so-called "network efficiency" that is useful in many cases is defined as follows:

$$E = \frac{1}{N(N-1)} \sum \frac{1}{d_{ij}}. \tag{9}$$

This quantity E is an indicator of the traffic capacity of a metro network, and avoids the divergence of the characteristic path length. It helps to explore how the topological properties of the SMN responded to different accidents in global scope. Metro systems with high network efficiency mean that travel should be fast and convenient under normal operating conditions. In weighted networks, it seems natural to generalize the notion of network efficiency through replacing the shortest paths with their weighted versions. The spatial attributes of the SMN are embodied in the physical spatial distance, measured in kilometers, characterizing each connection.

4 Results

4.1 Station vulnerability

In a complex transportation system, not all stations are equivalent. Conventional researchers usually regarded the degree centrality of a node as the only measurement for evaluating the significance of the node. In addition, betweenness is also an effective measurement of the global function of a node and has been used as a global geometric factor for node importance evaluation. However, there are few studies on node importance that is measured by damage rather than degree or betweenness.

Tables 2 and 3 show the percentage of functionality loss of the entire network when a station is removed from the network. As shown in Tables 2 and 3, the station with the largest strength and betweenness in the SMN is People's Square, which has six edges connecting to other stations and undertakes nearly 0.7 million passengers on morning rush hours. However, its damage value of the largest connected cluster (LCC^w) and global network efficiency (GNE) is 5.00 and 3.71%, which are both lower than Shanghai Railway Station, Caoyang Road and Zhenping Road. The station resulting in the largest damage of LCC^w in the SMN is Shanghai Railway Station, whose damage is 6.58%, implying that 6.58 percent of passenger flows rely on Shanghai Railway Station, which is their unique choice to connect to other stations.

The top ten stations with the largest damage of LCC^w and network efficiency are shown in Table 4. The damage of LCC^w depicts the level that the network is divided. Generally speaking, the removal of one node will not have a great influence on the integrity of the network. But, it can be seen from Table 4 that the network disintegrates into smaller sub-networks, disconnected parts because of the closure of station, which would have a major effect on regular operations of SMN. Of these, the most serious one is Shanghai Railway Station, which would affect about 6.58%

Table 2 Top 10 stations with the largest strength

Rank	Node name	Damage of LCC^w (%)	Damage of GNE (%)	Degree
1	People's Square	5.00	3.71	6
2	Xujiahui	3.67	2.71	6
3	Century Avenue	3.75	6.90	8
4	East Nanjing Road	2.96	2.22	4
5	Jing'an Temple	2.90	2.18	4
6	Shanghai Railway Station	6.58	7.60	4
7	Changshu Road	2.82	1.76	4
8	Zhongshan Park	2.68	2.61	4
9	Jiangsu Road	2.55	1.60	4
10	South Shaanxi Road	2.52	1.56	4

Table 3 Top 10 stations with the largest betweenness (weighted)

Rank	Node name	Damage of LCC^w (%)	Damage of GNE (%)	Degree
1	People's Square	5.00	3.71	6
2	Xujiahui	3.67	2.71	6
3	Century Avenue	3.75	6.90	8
4	Shanghai Railway Station	6.58	7.60	4
5	East Nanjing Road	2.96	2.22	4
6	Caoyang Road	6.05	8.56	4
7	Zhenping Road	5.38	8.29	4
8	Hailun Road	1.39	3.03	4
9	Oriental Sports Center	4.25	7.81	5
10	Changshu Road	2.82	1.76	4

of passenger flows. Meanwhile, it was found that stations connected radial metro lines and core areas usually result in serious damage of subgraph, such as Shanghai Railway Station, Yishan Road and Caoyang Road, as shown in Fig. 4. If such sorts of stations are temporarily off-line due to malicious attacks, the stations of radial lines away from central areas would lose contact with other stations in the network. Whereas for stations in the core areas, even the deletion of hub stations may not

Table 4 Top 10 stations with the largest damages

Rank	Node name	Damage of LCC^w (%)	Degree	Node name	Damage of GNE (%)	Degree
1	Shanghai Railway Station	6.58	4	Siping Road	9.64	4
2	Yishan Road	6.50	5	Caoyang Road	8.56	4
3	Caoyang Road	6.05	4	Zhenping Road	8.29	4
4	Zhenping Road	5.38	4	Oriental Sports Center	7.81	5
5	People's Square	5.00	6	Shanghai Railway Station	7.60	4
6	Guilin Road	4.74	2	Fengqiao Road	7.29	2
7	Shanghai South Railway Station	4.50	3	Yishan Road	7.07	5
8	North Zhongshan Road	4.42	2	Century Avenue	6.90	8
9	Oriental Sports Center	4.25	5	Langao Road	6.88	2
10	Fengqiao Road	4.20	2	Hongkou Football Stadium	6.76	4

cause disconnection and division of network and have a relatively small impact on the integrity of the network, such as Xujiahui. This phenomenon can also be explained by the metro network route. Taking Caoyang Road as an example, it serves as a link connecting Line 11 and downtown. If Caoyang Road was attacked, the stations located north of Caoyang Road had no other route to enter the inner city, which would lead to traffic congestion in Caoyang Road. Similarly, if Xujiahui was attacked, although many passengers would be affected, the remaining network could supply enough alternative route choices for passengers, so a large amount of passengers can still arrive at their destinations through other alternative routes.

Similar patterns were also observed in network efficiency and secondly, it is interesting to find that some stations that are highly connected, such as Century Avenue, Xujiahui, have relatively small damage values. In contrast, some stations with large damages, such as Guilin Road and North Zhongshan Road, have quite small degrees. These results reveal that transfer sites may not have much more influence than regular stations. It is different from conventional views that value transfer sites and undervalue regular stations. After a comprehensive investigation,

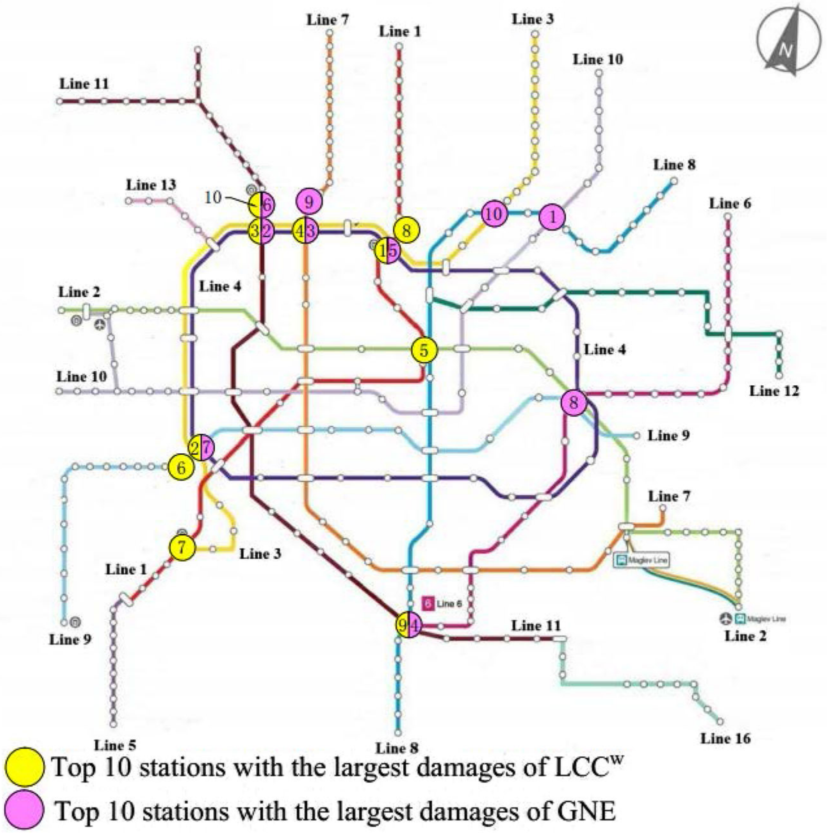


Fig. 4 Locations of stations with the largest damages of Shanghai metro

it was found that these kinds of regular stations can result in division of networks and deserve more attention. The above analysis provides a new perspective to examine the essentiality of a station and clearly shows that the essentiality of a station can be characterized by its damage, not just degree centrality or betweenness centrality.

4.2 Vulnerability of multiple stations failure

Accidents often affect more than one station. Firstly, the failure of a station may affect a continuous section and cause multiple stations failure at the same time. Secondly, terrorists often attack several metro stations simultaneously. For example, the July 7, 2005 London bombings, four Islamist extremists separately detonated three bombs in quick succession aboard London Underground trains across the city, and later, a fourth on a double-decker bus in Tavistock Square. On March 29, 2010, similar suicide bombings were carried out by two women during the morning rush hour, at two stations of the Moscow Metro (Lubyanka and Park Kultury). Thirdly, the impact of natural disasters also tends to spread to multiple stations. According to the characteristics of urban rail transit operation accidents, this section discusses the impact of multiple stations failure on the performance of SMN.

As seen in Table 5, multiple stations failure causes much more damage than a single station failure. In particular, the failure of five stations identified by the highest weighted betweenness i.e., People's Square, Xujiahui, Century Avenue, Shanghai Railway Station and East Nanjing Road, has affected about 37.63% of passenger flows and caused nearly 43.13% loss of global network efficiency. Secondly, multiple stations identified by the largest damages of LCC^{w} and GNE also have a great influence on the performance of SMN, indicating that these two approaches can also help identify the key node in the network. Besides, the damage caused by the highest weighted betweenness attack was significantly larger than that caused by the highest betweenness attack, which implies that the introduction of geographical space induces large betweenness centrality fluctuations and makes the hubs become more central.

As discussed in Sect. 4.1, stations identified by the functional loss could cause the largest damage on the SMN when a single station is attacked. But when multiple

Table 5 The influence of multiple stations failure on SMN performance

Index stations	Damage of LCC^{w} (%)	Damage of GNE (%)
Top 5 stations with the largest strength	18.05	22.27
Top 5 stations with the largest degree	22.01	27.55
Top 5 stations with the highest weighted betweenness	37.63	43.13
Top 5 stations with the highest betweenness	22.96	27.80
Top 5 stations with the largest damages of LCC^{w}	29.57	27.68
Top 5 stations with the largest damages of GNE	23.30	36.87

stations are under attack at the same time, the highest weighted betweenness is the most effective way to identify the crucial stations in the SMN. The presented results suggest that the transit managers cannot only think about the station local properties (such as passenger flows, the number of connected stations), but also its position and role in the metro network and the interplay between weight dynamics (passenger flow) and spatial constraints (geographical space).

4.3 Vulnerability of Shanghai Metro Network to different attacks

The vulnerability of the SMN is investigated in this section. As discussed in the previous section (see Sect. 3.3), several topological parameters including the weighted largest connected cluster, and network efficiency were applied to assess the changes of the characteristics for subjection to five different deletion strategies. Figure 5 portrays the changes in the weighted largest connected cluster subjected to four malicious attack strategies as well as random failures and the weighted largest connected cluster is calculated by using formula (5). As expected, all intentional attack strategies result in a rapid breakdown of the SMN with a very small threshold value of the fraction of removed stations, while the random failures result in the minimum damage among five different station failure modes. In addition to the initial phase, the damage caused by the highest weighted betweenness and topological betweenness attack is precisely the same, showing that they share the similar order of node removal. It is interesting to find that the LCC^w decreases faster upon removal of nodes with the highest betweenness instead of nodes with the largest strength and degree. This implies that it is more effective to destroy the SMN by deleting nodes which are identified as central according to global (i.e. betweenness) properties rather than local properties (i.e. degree, strength). Therefore, it is necessary to protect not only the hubs but also strategic points such as bridges and bottleneck structures in order to maintain the structural integrity

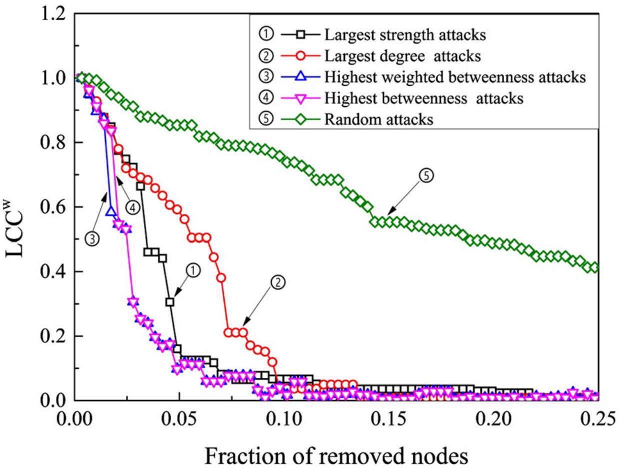


Fig. 5 The changes of LCC^w with different malicious attack strategies and random failures

of a network. Figure 4 also shows that the SMN is very fragile when subjected to malicious attacks, and it is robust against random failures.

The network efficiency is a better metric to measure the global connectivity of the network. Figure 6 shows the changes of the network efficiency for a metro network subject to four malicious attack strategies as well as random failures. With the increase of the fraction of the removed nodes, the network efficiency decreases when subjected to different attack rules. The highest betweenness attacks cause the maximum damage to the network and the highest weighted betweenness and topological betweenness attack also cause the same functionality loss to the network except the initial state, which probably implies that station spacing has less effect on the network than the one caused by passenger flows. Furthermore, the damage caused by the largest strength and largest degree attacks are slightly smaller than that caused by the highest betweenness attacks. The network efficiency can be preserved by random failures. So it can be known that the nodes with large betweenness and strength are more important than the nodes with small betweenness and strength to the connectivity of the network. Figure 5 also shows that the highest betweenness attacks will generate more isolated nodes than the other three malicious attack strategies. Therefore, according to Figs. 5 and 6, we can declare that the highest betweenness attack strategy is the most effective mode to destroy the SMN, so the nodes with high betweenness must be given more protection. This result is consistent with previous studies (Dall'Asta et al. 2006; Zhang et al. 2011). Certainly, the nodes with large strength are very important to the network, as the damage caused by the largest strength attacks is slightly lower than the damage caused by the highest betweenness attack.

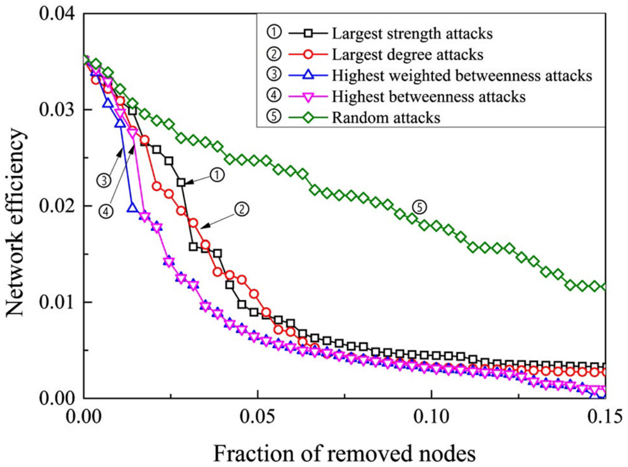


Fig. 6 The changes of the network efficiencies under malicious attacks and random failures

4.4 Comparison of weighted and topological networks vulnerability

Currently, most relevant studies in this field were conducted in the view of topology, which meant they considered each station as a simple node in graph theory. The traffic of a station and cost of travel time were rarely considered in previous literatures. It is therefore interesting to quantify the difference between weighted and topological networks vulnerability. As the global network efficiency varies with different networks, the relative size of the largest connected component is adopted to evaluate the vulnerability of weighted and topological networks. Figure 7 shows the behavior of LCC^w and LCC of all cases. Within this figure, WS represents the largest strength attack on the weighted network, WD the largest degree attack on the weighted network, WB denotes the highest betweenness (weighted) attack on the weighted network and WR denotes random failure on the weighted network. Similarly, TS, TD, TB and TR represent the largest strength attack on the topological network, the largest degree attack on the topological network, the highest betweenness (weighted) attack on the topological network and random failure on the topological network, respectively.

From Fig. 7, it is interesting to observe that the functionality decrease of weighted networks caused by intentional attack strategies is even faster and more pronounced than thought by considering only topological properties. This indicates that the purely topological measure of the relative size of the largest connected subgraph does not convey all the information of a real-world network. In other words, the functionality of a metro network could be temporarily endangered in terms of passenger flows even though the physical structure of the network is still globally well-connected. This implies that weighted networks are more fragile than topological networks when subject to malicious destructions. All intentional attack strategies are very effective in damaging the network, reaching the complete destruction at a very low level of removed nodes. As seen in Fig. 6, the maximum

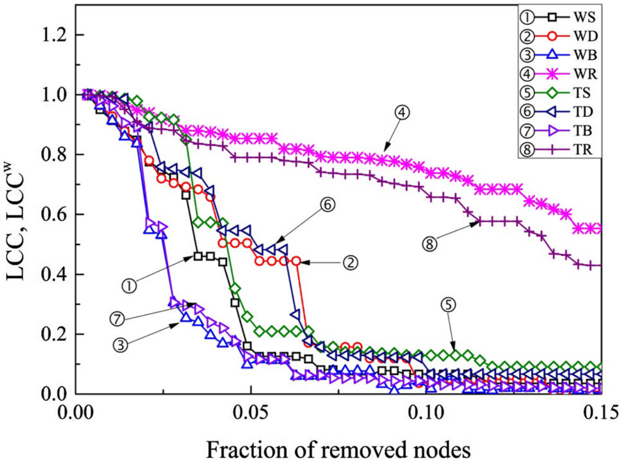


Fig. 7 Effect of malicious attacks and random failures on weighted and topological network

damage is still achieved by the highest betweenness attack which leads to a very fast decrease of the giant component size both for topological and weighted networks. Whereas, the network may unfortunately be damaged by using attack strategies based on local quantities (i.e. degree, strength) which are more easily obtained and calculated. Figure 5 also shows that the random failure causes slightly more damage to the weighted network than the topological network. This is probably due to a few hub stations dominating their topology and traffic, such as People's Square and Xujiahui. Any node that fails probably has small degree and strength (like most nodes), which is expendable and has less effect on the structural integrity and functionality of a weighted network. The flip side is that the weighted networks are vulnerable to intentional attacks on the hub station. Despite the existence of a few highly connected nodes (hubs) which leave the network vulnerable to attacks, a decentralized network structure and high redundancy may help to improve robustness and network efficiency under normal circumstances or in the case of failures.

5 Discussion

5.1 Improving robustness of a metro network against failures

In the modern society, it is known that transit networks have a significant impact on the city, so more attention should be paid on the robustness of a metro network. In other words, the planning of the topological structure is a critical issue of great operational significance for a subway system (Yang et al. 2015). In this study, the topological features and sensitivity of the SMN to random failures and malicious attacks were investigated. The failure tolerance and attack vulnerability were measured by the relative size of a large component and global network performance. Quantitative results in Sect. 4.1 show that the SMN is robust against random failures but fragile for malicious attacks. In addition, the highest betweenness attack protocol is the most effective mode to destroy the SMN. Then, it is natural to ask how to improve the robustness of a metro network. General solutions seem to protect the crucial stations in metro systems and build more interchange stations. However, the positions and the number of interchange stations deserve to be further discussed. The backbone network of the Shanghai Metro System had been well constructed and entered a new era of networking operation. Its network structure will not change significantly and the robustness of these metro networks can be only improved by adding new links and optimizing the network structure.

According to research by Motter and Lai (2003), it is found that the heterogeneity of the networks makes them particularly vulnerable to attacks in that a largescale cascade may be triggered by disabling a single key node. In turn, the hub nodes and load are distributed very evenly in the network, resulting in the high robustness against failures. This finding could be illustrated by our contrastive analysis of weighted and topological network. It is interesting to observe that all intentional attack strategies are very effective in damaging the network (both weighted and topological) and the weighted version of SMN is more vulnerable than its topological network when subjected to intentional attacks. This implies that the current topological network of SMN is heterogeneous and the introduction of passenger flow exacerbates the heterogeneity of the networks. Thus, traditional transit planners should not only consider such characteristics as demography, geography, demand, cost and others, but also the layout and structure of a network. The layout of Tokyo Metro provides good experience for Shanghai Metro. It has 13 lines (of all types), with 215 stations; 58 of these stations are transfers, hence a ratio of 26.98%, which is significantly high. All lines intersect at multiple points, resulting in that interchange stations distribute evenly throughout the whole system and load on each line is approximately equal. These span-uniform interchange stations enable the metro to offer sufficient alternative routes for passengers when subject to attacks. Furthermore, the well-distributed transfer stations and lines ensure that a local disruption cannot impair the global structure of a metro system severely. Thus, it can improve the network robustness against failures by making the network structure and passenger flow more homogeneous.

The exposure of the stations has been obtained from data on criticality. As seen in Fig. 6, over half of the top 10 stations locate on or next to the circular line (line 4), indicating that the circular line plays an important role in the SMN. It serves as the link between urban and rural areas and provides multiple alternative routes. Circular lines play a key role in the metro network because it is the most effective way to create new transfer stations that will further increase the connectivity and robustness of a network. In this regard, transit planners and managers can consider to build another circle line or (semi)-circle line to connect peripheral regions and relieve heavy stress of crucial stations on line 4.

The results obtained are also of high interest in metro operation and management. For a single station, the functional loss of the metro network is the most effective and direct method to identify crucial stations. While multiple stations are attacked simultaneously, the highest weighted betweenness attack causes the largest damage to the SMN. Therefore, under a constrained budget, the policymakers should consult the ranking of crucial stations in different situations, which will allow them to prioritize the allocation of financial and other constrained resources. For example, metro operators and relevant government agencies may decide to protect the top one to five vulnerable stations, depending on the amount of available resources.

According to our results and previous research (Zhang et al. 2011), the highest betweenness attack protocol is the most effective mode to destroy the whole SMN. This evidence brings both good and bad news concerning the protection of large-scale metro systems. On one hand, the planning of an effective targeted attack only needs to gather information on the initial state of the network. On the other hand, the identification of crucial nodes to protect is an easier task that somehow is weakly dependent on the attack sequence. As a consequence, the stations with high betweenness must be given more protection.

5.2 Generality and future work

The vulnerability of a metro network against various malicious attack strategies and random failures is an extremely complicated issue, and comprehensive studies are required to be carried out by combining relevant scientific theory. This paper aims to investigate the underlying relationship between the structure of the SMN and its vulnerability by introducing complex network theory. Several traffic characteristics such as passenger flows, station spacing are considered in the study of the vulnerability of weighted networks to different malicious attack strategies, and simulation results show that weighted complex networks are more fragile than expected through comparative analysis with topological networks. Although only taking the SMN as an example, this investigation and the practice are possible to be applied to the network design and safety management of other large-scale metro systems. Note that different metrics used for node removal scenario analysis will have different rank order for the most important nodes in the network, so it is difficult to say which is more crucial. So it should use these different metrics case by case. The current results could supply a systematic and detailed case for future research, which can be incorporated into more complex networks such as bus transport. Besides, the capacity of station and dynamic traffic redistribution after failures and attacks should be considered and further studied in order to assess the vulnerability of a metro network more accurately.

6 Conclusion

To summarize, this paper investigates the vulnerability of a weighted metro network with traffic and geographical space by using complex network theory, aiming to find reasonable measures to improve the robustness of metro systems. The Shanghai metro, a typical resource of metro network research, is taken as an example to examine how a metro system responds to four malicious attack strategies as well as random failures and how traffic and spatial constraints influence the system's robustness.

1. The study of the vulnerability of weighted networks to various malicious attack strategies and random failures shows that the SMN is robust against random failures but fragile for malicious attacks and the highest betweenness attack strategy causes the most damage to SMN among four attack modes. In addition, when the traffic characteristics are taken into account, the weighted metro network becomes more fragile than expected from the comparison with topological quantities and the structural integrity of the weighted network is vanishing before the topological network is fragmented.
2. A new indicator for node importance evaluation is proposed, which could apply to identify hubs, bridges and bottlenecks for a metro network.
3. For a single station, the functional loss of the metro network is the most effective and direct method to identify crucial stations. While multiple stations are attacked simultaneously, the highest weighted betweenness attack causes the largest damage to the SMN. Therefore, under a constrained budget, the policymakers should consult the ranking of crucial stations in different situations, which will allow them to prioritize the allocation of financial and other constrained resources.

4. Circular lines play a key role in the metro network because it is the most effective way to create new transfer stations that will further increase the connectivity and robustness of a network. In this regard, transit planners and managers can consider building another circle line or (semi)-circle line to connect the current lines and improve the network efficiency.

Although this work could make a contribution to the assessment of the vulnerability of the metro system, due to the limitation of the passenger flow, the analysis of metro network vulnerability is only based on the analysis over the SMN and exposes several insufficiencies. In our further research, the dynamic vulnerability analysis of metro systems, a corresponding study of passenger flows, the frequency of threat occurrence and the mechanism of network disruption, would integrate with the current work to provide an improved risk assessment model and safety management strategies for metro systems.

Acknowledgements The authors thank the Shanghai Shentong Metro Company, for providing valuable information about the SMN for academic and research activities. In addition, the authors acknowledge the financial support of Project 71671127 by the National Natural Science Foundation of China.

References

Albert R, Barabási A-L (2002) Statistical mechanics of complex networks. Rev Mod Phys 74:47–97

Angeloudis P, Fisk D (2006) Large subway systems as complex networks. Physica A 367:553–558

Berche B, von Ferber C, Holovatch T, Holovatch Y (2009) Resilience of public transport networks against attacks. Eur Phys J B Condens Matter Complex Syst 71(1):125–137

Berche B, von Ferber C, Holovatch T, Holovatch Y (2010) Public transport networks under random failure and directed attack. Dyn Socio-Econ Syst 2(2):42–54

Berdica K (2002) An introduction to road vulnerability: what has been done, is done and should be done. Transp Policy 9:117–127

Berdica K, Mattsson LG (2007) Vulnerability: A Model-Based Case Study of the Road Network in Stockholm. In: Murray AT, Grubesic TH (eds) Critical Infrastructure. Advances in Spatial Science. Springer, Berlin, Heidelberg, pp 81–106

Boccaletti S, Latora V, Moreno Y, Chavez M, Hwang DU (2006) Complex networks: structure and dynamics. Phys Rep 424(4–5):175–308

Bruyelle JL, O'Neill C, El-Koursi EM, Hamelin F, Sartori N, Khoudour L (2014) Improving the resilience of metro vehicle and passengers for an effective emergency response to terrorist attacks. Saf Sci 62:37–45

Cats O, Jenelius E (2012) Vulnerability analysis of public transport networks: a dynamic approach and case study for Stockholm. In: The international symposium on transportation network reliability

Cats O, Yap M, Oort NV (2015) Exposing the role of exposure: identifying and evaluating critical links in public transport networks. In: The international symposium on transportation network reliability

Chopra SS, Dillon T, Bilec MM, Khanna V (2016) A network-based framework for assessing infrastructure resilience: a case study of the London metro system. J R Soc Interface 13(118):20160113

Crucitti P, Latora V, Marchiori M, Rapisarda A (2003) Efficiency of scale-free networks: error and attack tolerance. Physica A 320:622–642

Dall'Asta L, Barrat A, Vespignani L (2006) Vulnerability of weighted networks. J Stat Mech: Theory Exp 25(04):04006

De-Los-Santos A, Laporte G, Mesa JA, Perea F (2012) Evaluating passenger robustness in a rail transit network. Transport Res Part C Emerg Technol 20(1):34–46

Derrible S, Kennedy C (2010) The complexity and robustness of metro networks. Physica A 389(17):3678–3691

Ghedini CG, Ribeiro CH (2011) Rethinking failure and attack tolerance assessment in complex networks. Physica A 390:4684–4691

Guimerá R, Amaral LAN (2004) Modeling the world-wide airport network. Eur Phys J B Condens Matter Complex Syst 38(2):381–385

Han Y, Cheng H, Zhao X, Xue X (2012) Theoretic structure of urban mass transit operation safety based on vulnerability. Urban Mass Transit 15:15–19

Kyriakidis M, Hirsch R, Majumdar A (2012) Metro railway safety: an analysis of accident precursors. Saf Sci 50:1535–1548

Kyriakidis M, Hirsch R, Majumdar A (2014) A global safety analysis and best practice for metro railways. Soc Sci Electron Publ 166(6):362–374

Laporte G, Mesa JA, Perea F (2010) A game theoretic framework for the robust railway transit network design problem. Transport Res Part B Methodol 44(4):447–459

Luathep P, Sumalee A, Ho HW, Kurauchi F (2011) Large-scale road network vulnerability analysis: a sensitivity analysis based approach. Transportation 38(5):799–817

Mattsson LG, Jenelius E (2015) Vulnerability and resilience of transport systems—a discussion of recent research. Transport Res Part A Policy Pract 81:16–34

Motter AE, Lai Y-C (2003) Cascade-based attacks on complex networks. Phys Rev E: Stat Nonlinear Soft Matter Phys 66(6):114–129

Nawrath C (2006) Unraveling the complex network of cuticular structure and function. Curr Opin Plant Biol 9(3):281–287

Newman ME, Strogatz SH, Watts DJ (2001) Random graphs with arbitrary degree distributions and their applications. Phys Rev E 64:026118

Ouyang M, Zhao L, Hong L, Pan Z (2014) Comparisons of complex network based models and real train flow model to analyze Chinese railway vulnerability. Reliab Eng Syst Saf 123(3):38–46

Perea F, Puerto J (2013) Revisiting a game theoretic framework for the robust railway network design against intentional attacks. Eur J Oper Res 226(2):286–292

Petter H, Beom Jun K, No YC, Seung Kee H (2002) Attack vulnerability of complex networks. Phys Rev E 65(5):056109

Riedel HU (2014) Chinese metro boom shows no sign of abating. Int Railw J 54(11):46–48

Rodríguez-Núñez E, García-Palomares JC (2014) Measuring the vulnerability of public transport networks. J Transp Geogr 35:50–63

Sienkiewicz J, Hołyst JA (2005) Statistical analysis of 22 public transport networks in Poland. Phys Rev E Stat Nonlin Soft Matter Phys 72(4 Pt 2):046127

Taylor MAP, D'Este GM (2007) Transport network vulnerability: a method for diagnosis of critical locations in transport infrastructure systems. Critical infrastructure. Springer, Berlin, pp 9–30

von Ferber C, Holovatch T, Holovatch Y, Palchykov V (2007) Network harness: metropolis public transport. Physica A 380(7):585–591

Wang J (2013) Robustness of complex networks with the local protection strategy against cascading failures. Saf Sci 53:219–225

Wang J, Fang W (2014) A structured method for the traffic dispatcher error behavior analysis in metro accident investigation. Saf Sci 70:339–347

Wang J, Mo H, Wang F, Jin F (2011) Exploring the network structure and nodal centrality of China's air transport network: a complex network approach. J Transp Geogr 19(4):712–721

Wang H, Huang J, Xu X, Xiao Y (2014) Damage attack on complex networks. Physica A 408:134–148

Xu Z, Sui DZ (2007) Small-world characteristics on transportation networks: a perspective from network autocorrelation. J Geogr Syst 9(2):189–205

Xu X, Hu J, Liu F (2007a) Scaling and correlations in three bus-transport networks of China. Physica A 374(1):441–448

Xu X, Hu J, Liu F (2007b) Empirical analysis of the ship-transport network of China. Chaos 17(2):471–516

Yang Y, Liu Y, Zhou M, Li F, Sun C (2015) Robustness assessment of urban rail transit based on complex network theory: a case study of the Beijing subway. Saf Sci 79:149–162

Yuan J, Li Q, Jia R, Wang Z (2012) Analysis of operation vulnerabilities of urban metro network system. China Saf Sci J 22:92–98

Zhang J, Xu X, Hong L, Wang S, Fei Q (2011) Networked analysis of the Shanghai subway network, in China. Physica A 390(23):4562–4570

Zhang J, Xu X, Hong L, Wang S, Fei Q (2012) Attack vulnerability of self-organizing networks. Saf Sci 50:443–447

Zhou Z, Irizarry J, Li Q (2014) Using network theory to explore the complexity of subway construction accident network (SCAN) for promoting safety management. Saf Sci 64:127–136