Available online at www.ijpe-online.com

International Journal of Performability Engineering

vol. 15, no. 10, October 2019, pp. 2762-2771
DOI: 10.23940/ijpe.19.10.p23.27622771

Robustness Analysis of Urban Rail Transit Network

Hui Xu[a,b,*] and Yang Li[a]

[a]*School of Economics and Management, Chongqing University of Posts and Telecommunications, Chongqing, 400065, China*
[b]*Department of Building, School of Design and Environment, National University of Singapore, 4 Architecture Drive, 117566, Singapore*

Abstract

The urban rail transit system is threatened by various kinds of risk events, so it is necessary to explore system robustness and guarantee safe operation. Considering the overall topological structures of urban rail transit network (URTN), the complex network theory is adopted. After calculating the topological parameters and robustness analysis parameters, the attack strategies for URTN are established. The proposed methodology is applied to the Singapore Mass Rapid Transit System. The results demonstrate that malicious attacks have more serious impacts on system robustness than random attacks. In addition, the nodes that link to different sections of the network, connect a cluster of nodes to the main network, or connect to more than one rail transit line are identified as important nodes of the network. The obtained results could supply valuable references for the safety management of URTN. The proposed methodology could also be used for other URTN robustness analyses.

Keywords: robustness; urban rail transit network; complex network; system safety

(Submitted on August 14, 2018; Revised on September 15, 2018; Accepted on October 25, 2018)

1. Introduction

Urban rail transit is becoming the main stream of public transportation and plays a significant role in people's daily travel [1]. Several rail transit lines have been constructed in many metropolises and countries, such as New York, Beijing, and Singapore, resulting in complex subway networks that possess intricate inter-station coupling relationships and high station densities [2]. The importance of urban rail transit can be observed from the large passenger capacity, high transportation efficiency, environmental impact, and more [3]. However, the frequent occurrence of risk events due to unreasonable planning, insufficient collaborative management measures, malicious attacks, natural hazards, etc. has attracted the attention of governments and scholars [2]. Considering the primary function of a rail transit system is to facilitate the mass movement of passengers and goods from origins to destinations across a network, any disruption of the rail transit network components could influence the normal operation of the entire system [4]. Risk events such as electrical failures, train breakdowns, and engineering failures may lead to temporary operation closure in one or both directions, and incidents such as suicides, strikes, or demonstrations may also affect the operation of the rail transit network. More dramatic events like terrorist attacks would have particularly far-reaching and long-lasting effects on the network [5]. In particular, due to various stations located in different positions of the network, the disruption of the stations could influence the entire rail transit network differently. Accordingly, in order to guarantee the efficient running of the rail transit network, the robustness of the network should be analyzed and some important nodes of the network with high vulnerability should be identified, which are the focuses of this research.

Robustness means the quality of being strong and healthy or unlikely to break or fail. Robustness of a rail transit network is determined with respect to different accidental behaviours, which are associated largely with system reliability and variability, and is a design criterion of the system. Specifically, it is an ability of a rail transit network to withstand unexpected risk events with an acceptation reduction of operation performance and maintain the partial characteristics in face of disruptions to its network components [2]. This ability tends to measure the amount of stress that can be absorbed before system failure [6]. Considering the various kinds of risks in the urban rail transit network (URTN), this research

* Corresponding author.
E-mail address: xuhui@cqupt.edu.cn

explores the robustness for the rail transit network.

Understanding the topological characteristics of a rail transit network is crucial for improving the robustness of the stations in the network against the inside disruptions and outside attacks [7]. Complex network theory has been used to study the safety management of rail transit system in many studies [2, 8-9]. Several attributes for applying complex network theory include the following points: (1) the rail transit network presents obvious scale-free network characteristics that most nodes in the scale-free network have exponents between 2 and 3 and lack a characteristic degree or scale, while only a small number of nodes have high connectivity, called hubs [10]; (2) conventional applications of complex network to various infrastructures, including grid networks, aviation networks, pipelines, and the Internet, have proven that the complex network theory has the potential to be used at different network scales; (3) risk events occurring in the rail transit system in recent years have demonstrated that risk events in hub stations would lead to some dysfunctions or operation adjustments for the rail transit system. The above three attributes provides reasonable accordance to explore rail transit networks from a complex network theory perspective.

In this study, the complex network theory is adopted and the Singapore Mass Rapid Transit System (SMRT) is used for the case study. The research is organized as follows. The second section is the literature review. In the third section, the methodology, including the complex network, topological parameters, robustness analysis parameters, and attack strategies for the URTN are illustrated. The fourth section demonstrates the case study of Singapore Mass Rapid Transit System (SMRT) and the detailed implementation steps of the proposed methodology. Discussion and conclusion for this research are presented in the last two sections.

2. Literature Review

The robustness of rail transit networks has been investigated based on network topological characteristics in many studies. The world's largest subway systems were analysed, and the results showed that the networks are robust to random attacks due to the characteristics of high connectivity and low maximum vertex degree [11]. Network science methodologies were applied to the robustness of metros by looking at 33 metro system worldwide, and it was demonstrated that most metros are scale-free and small-worlds [8]. A methodology for measuring public transport network vulnerability was developed, including the considerations for lines and circular lines. The real trips distribution was used, and every link of the network was measured criticality [5]. The robustness assessment of urban rail transit was conducted based on complex network, and the topological properties of the rail transit network were quantitatively analyzed [12]. By using the network science and graph theory, ten theoretical and four numerical robustness metrics and their performance in quantifying the robustness of real metro networks were investigated [6]. The integrated accessibility and reliability indicators were proposed to evaluate a rail transit network's performance by analyzing the topologies of the network, and the dynamics of the network performance in four evolutionary stages were considered [13].

Some cases were employed in existing research, such as the Seoul metro transit system, the Madrid metro system, and the Beijing rail transit system. The robustness of urban rail transit was assessed based on complex network theory. The topological properties of the Beijing rail transit system were quantitatively analyzed through a mathematical statistical model, and the results show the typical scale-free network characteristics of the system [2]. Similarly, the statistical topology parameters of the Beijing rail transit network were quantitatively analyzed based on complex network theory [1]. The results revealed that the threshold of loop line damage is smaller than a straight line when under attack, and the failure is difficult to control when attacking the loop line. For the Shanghai rail transit network, the reliability and robustness of the network were analyzed by using the topological parameters, and two novel parameters called the functionality loss and connectivity of subway lines were proposed [14]. A vulnerability analysis of the Shanghai metro network was also conducted, and it showed that the stations with a high degree are more significant in maintaining the network size, while the stations with large betweenness are critical to network efficiency and connectivity [15]. A resilience method integrating the network topological and passenger volume characteristics of rail transit network was demonstrated under daily operational risk events, and the results revealed that the identification of the critical stations depends on the duration time of different risk events and the characteristics of the stations [16]. The metro network vulnerability was proposed from the perspective of line operation and indicated that (1) the metro lines with a large number of passengers have a significant influence on the network vulnerability, and (2) the circle line could have an important impact on passenger flow re-distribution in case of emergency [17]. In addition, the networked characteristics of three metro networks (Beijing metro network, Shanghai metro network, and Guangzhou metro network) were analysed, and two malicious attacks were used to investigate the vulnerability of metro networks [18].

The existing research considers the topological characteristics of rail transit networks, providing useful reference for this research. The robustness of networks was explored by using complex network in this research. Taking the Singapore

mass rail transit network as an example, multiple attack scenarios for the network were considered. The robustness parameters of the network under different scenarios were measured. The risky scenarios proposed in this research present the innovative features and could be adopted in rail transit practical management.

3. Methodology

3.1. Construction of URTN

In a complex network model, the components of a system are often defined as vertices, and the interactions among vertices are edges [19-20]. 20 networks have been constructed based on the complex network theory for the world's largest subways [11]. The network characteristics, including high connectivity, low maximum vertex degree, and typical features of small-world and scale-free categories, are presented.

According to complex network theory, stations in the URTN could be virtualized as nodes, and tracks connecting two station directly could be virtualized as edges [15, 20]. The URTN could be viewed as an undirected graph, because urban rail transit generally has two-way traffic. The undirected graph is defined as $G = \langle V, E, A \rangle$, where $V = \left\{ v_i \middle| i = I \triangleq \{1, 2, \cdots, N\} \right\}$ is the set of network nodes and $E = \left\{ e_{ij} = (v_i, v_j) \middle| i, j \in I \right\} \subseteq V \times V$ is the set of network edges between two nodes. $A = [a_{ij}]_{N \times N}$ is the network adjacency matrix, where a_{ij} is defined as

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

Furthermore, assume $a_{ii} = 0$ for all $i \in I$. Because the graph is undirected, $e_{ij} \in E \prec\!\!=\!\!\succ e_{ji} \in E$, and thus the adjacency matrix A is symmetric and nonnegative [9]. The network adjacency matrix is established according to the operation situation of the URTN. The network could be constructed by inputting the adjacency matrix into the software UNINET.

3.2. Topological Parameters of URTN

3.2.1. Degree and Degree Distribution

In the context of URTN, degree k_i refers to the number of lines connected to station i and represents the local property of the station. The higher the degree, the more lines the station connects to, and the higher the interactive ability of the station. The degree distribution P_k means the probability of a node with degree k, which is a probability distribution function over the whole node [22].

3.2.2. Betweenness

The betweenness B_i of the node v_i is the number of shortest paths among all pairs of nodes passing through the node, which is the measurement of the nodes as a "bridge" and reflects the load of the node.

3.3. Robustness Analysis Parameters of URTN

3.3.1. Network Efficiency

Network efficiency demonstrates the average closeness of every node in the network. The higher the closeness, the shorter the distance between nodes, and the higher the efficiency. The network efficiency is defined as

$$E = \frac{1}{N(N-1)} \sum_{i \neq j \in I} \frac{1}{d_{ij}} \tag{2}$$

Where N is the number of nodes in the network and d_{ij} denotes the length of the shortest path between node i and node j. The value of E ranges from 0 to 1. $E = 1$ represents the URTN being an overall coupled network. In this

condition, the network has the highest connectivity and highest ability to provide alternative paths when attacked. $E=0$ represents all nodes in the network being isolated. In this condition, the connectivity of the network is the lowest, and the ability to provide alternative paths is zero. Thus, the network is the least robust.

3.3.2. Connectivity

Connectivity demonstrates the connection intensity of the network. The higher the intensity of the network, the higher the connectivity of the network, and the lower the influence of the risk events on the network. The connectivity is defined as

$$\sigma = \frac{TE}{N(N-1)} \tag{3}$$

Where TE is the number of true edges. Also, the value of σ ranges from 0 to 1. Similar to the network efficiency E, $\sigma=1$ represents the URTN being an overall coupled network. In this condition, the network has the highest connectivity and highest ability to provide alternative paths when attacked. $\sigma=0$ represents all the nodes in the network being isolated. The connectivity of the network is the lowest, and the ability to provide alternative paths is zero. In this condition, the network is the least robust.

3.3.3. Relative Size of the Maximal Connected Subgraph (*RSMCS*)

H is a maximal connected subgraph of G. The relative size of the maximal connected subgraph is defined as

$$S = \frac{N'}{N} \tag{4}$$

Where N' is the number of nodes of H. The value of S ranges from 0 to 1. $S=1$ indicates that the network has not been attacked, and $S=0$ indicates that the network crashes after been attacked. For the value of S, the closer to 1, the higher the ability to provide alternative paths of the network after risk event attacks; conversely, the closer to 0, the lower the ability to do so.

3.4. Attack Strategies for the URTN

The rail transit network may encounter two types of attacks, random attacks and malicious attacks. The common behaviours of the two types of attacks are shown in Table 1 [2].

Table 1. Common behaviours of random attacks and malicious attacks

Categories	Precursors	Description
Random attacks	Technical malfunctions	Broken rail, broken wheels, brake failure, gear failure, signal failures, power failure, crack rail, line fault, derailment caused by exceeding speed, train collision
	Passengers actions	Congestion, suicide in platform, fall onto track, falls on escalators, group fighting, unconscious destruction due to drunkenness, smoke in station/train, wrong operation by driver, passenger carrying dangerous goods, passenger carrying pets, riot caused by rumors, caught in train doors
	Management actions	Temporary disruption of service, temporary line maintenance, temporary closure for safety inspection, temporary closure for special activity, decision error
Malicious attacks	Targeted destruction	Deliberate destruction, passenger carrying dangerous/flammable goods, passenger carrying poisonous goods, kidnapping, trespass, manual destruction on rail, manual destruction on train, explosion in purpose, set fires, gun shooting, derailment caused by human, deliberate assassination to raise riot, etc.

Both categories of attack could lead to the disruption of operation. In the network simulation, the operation of the attacked station is disrupted and the station will be an isolated node in the network. For example, the station A in Figure 1 is attacked, and the connections around station A will be removed.

3.4.1. Random Attack Strategies

As for random attacks, the function "=RANDBETWEEN(bottom, top)" was used to generate a random number, which represents an attacked node in the rail transit network. The random attack includes the following two strategies:

- Independent attack: randomly attack one node in a one-time attack, and attack a total of five times;
- Continuous attack: randomly attack one node, and continuously attack one more node station until a total of five nodes are attacked.

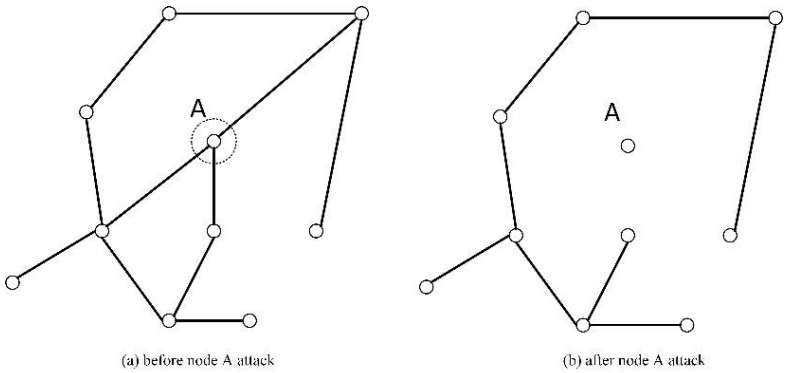

Figure 1. Structures of the connected graph before and after node attack

Independent attacks consider only one station in the URTN to be attacked. This corresponds with the real condition that one station in the URTN fail to work. Continuous attacks aim to simulate the continuous random failure of some stations. This condition may exist after natural hazards, such earthquakes or floods.

3.4.2. Malicious Attack Strategies

For malicious attacks, the nodes with high degrees and high betweenness are targets of attack. Malicious attacks include the following two strategies:

- Attack 1-5 nodes with high degree;
- Attack 1-5 nodes with high betweenness.

The attacked nodes are determined according to the calculated values of degree and betweenness. These nodes are special nodes in the network. The two strategies simulate the failure conditions after the above special nodes are attacked, which is meaningful for guiding the protection measure establishment in management practice.

4. Case Study of Singapore Mass Rapid Transit System

4.1. Basic Network Information

In 1987, the Singapore Mass Rapid Transit System (SMRT) begins operations with inaugural service between Yio Chu Kang station and Toa Payoh station on the North-South line. After 32 years of development, the SMRT system includes Mass Rapid Transit (MRT) and Light Rail Transit (LRT). In total, the system operates eight lines and 158 stations and carries more than two million passengers daily [23]. In the eight lines, the five MRT lines are the East West Line (Green Line), North South Line (Red Line), North East Line (Purple Line), Circle Line (Yellow Line), and Downtown Line (Blue Line). The three LRT lines are the Bukit Panjang LRT, Sengkang LRT, and Punggol LRT. Among the 158 stations, there are 25 transfer stations, including one station for three lines' transfer and 24 stations for two lines' transfer. According to the method illustrated in Section 3.1 and the condition of the SMRT network, the network model was constructed by using UCINET, as shown in Figure 2.

4.2. Topological Characteristics of the Network

4.2.1. Degree and Degree Distribution

The degrees of nodes in the SMRT network were calculated by using UCINET, as shown in Figure 3. It can be seen that the highest node degree is 6 and the average value of the node degrees is 2.27. The proportion of nodes with degree value 2 is 79.1%, which indicates that most stations in the SMRT network connect to two other stations.

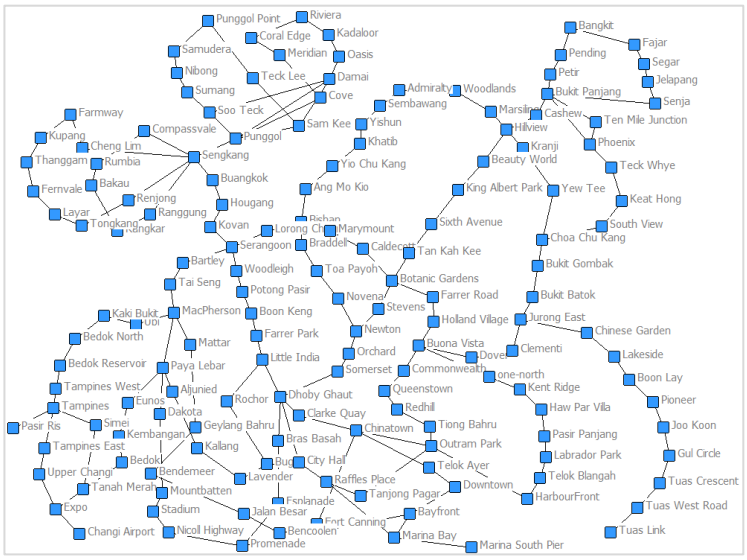

Figure 2. Singapore's Mass Rapid Transport (SMRT) network model

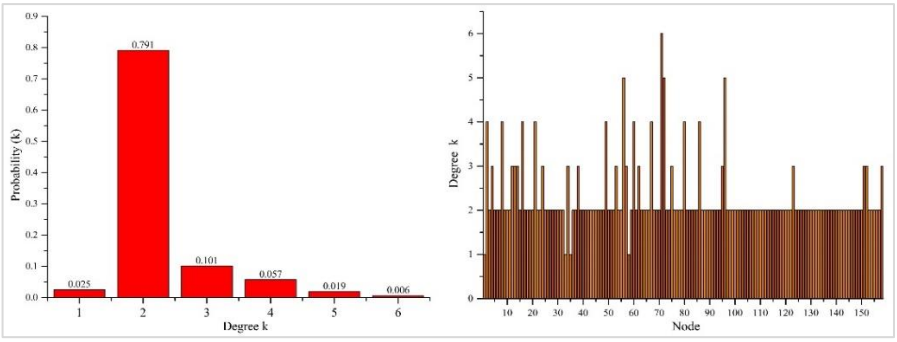

Figure 3. Degree and degree distribution of nodes in SMRT network

4.2.2. Betweenness

The betweenness of nodes in the SMRT network were calculated by using UCINET, and the nodes with top 20 betweenness values are shown in Table 2. The station Serangoon possesses the largest betweenness value, 5789, indicating that 5789 shortest paths within the network pass the station [15], followed by Bishan, Kovan, Botanic Gardens, and Sengkang.

Table 2. Nodes in the SMRT network with the top 20 betweenness

NO.	Node	Betweenness	NO.	Node	Betweenness
1	Serangoon	5789	11	Caldecott	2777
2	Bishan	4134	12	Buona Vista	2633
3	Kovan	3906	13	Bartley	2561
4	Botanic Gardens	3883	14	Tai Seng	2501
5	Sengkang	3855	15	Punggol	2030
6	Hougang	3810	16	Dhoby Ghaut	2025
7	Lorong Chuan	3720	17	Jurong East	1932
8	Buangkok	3712	18	Tan Kah Kee	1923
9	MacPherson	2823	19	Paya Lebar	1917
10	Marymount	2782	20	Farrer Road	1904

4.3. Robustness Analysis for the Network

4.3.1. Random Attack Simulation

The function "=RANDBETWEEN(1, 158)" was firstly used to generate the random attack nodes in the network. Five node numbers were generated, which are 62, 94, 61, 128, and 95. The representativeness of the five nodes are 62 (Little India), 94 (Telok Blangah), 61 (Clarke Quay), 128 (Segar), and 95 (Bayfront). Then, the simulations for the independent attack and continuous attack were implemented. After the random attack simulation, the three robustness assessment parameters for

URTN, network efficiency, connectivity, and RSMCS were calculated. The calculation results and the decrease rates are shown in Table 3 (network efficiency), Table 4 (connectivity), and Table 5 (RSMCS).

4.3.2. Malicious Attack Simulation

Malicious attacks were implemented for the nodes with high degree values and betweenness values. According to the calculation results of the two parameters, four nodes with the top four degree values (>= 5) and six nodes with top six betweenness values (>= 3800) are the targets of attack. The ten nodes are 71 (Sengkang, degree = 6), 56 (Dhoby Ghaut, degree = 5), 72 (Punggol, degree = 5), 96 (Bukit Panjang, degree = 5), 67 (Serangoon, betweenness = 5789), 49 (Bishan, betweenness = 4134), 68 (Kovan, betweenness = 3906), 86 (Botanic Gardens, betweenness = 3883), 71 (Sengkang, betweenness = 3855), and 69 (Hougang, betweenness = 3810). After the malicious attack simulation, the three robustness assessment parameters for URTN, network efficiency, connectivity, and RSMCS were calculated. The calculation results and the decrease rates are shown in Table 3 (network efficiency), Table 4 (connectivity), and Table 5 (RSMCS).

5. Discussion

The discussion for the robustness assessment results after the random attack and malicious attack was conducted from two angles: (1) horizontal analysis and (2) longitudinal analysis.

5.1. Horizontal Analysis

The horizontal analysis was conducted for every parameter's calculation result, comparing between random attack and malicious attack.

5.1.1. Horizontal Analysis for the Network Efficiency

The network efficiency and the decrease rates after the random attack and malicious attack are shown in Table 3.

Table 3. The network efficiency and decrease rates after the two types of attacks

Random attack nodes	Original network	62	94	61	128	95	62	62→94	62→94 →61	62→94 →61→128	62→94 →61→128→95
Network efficiency	0.1260	0.1224	0.1238	0.1231	0.1238	0.1237	0.1224	0.1203	0.1179	0.1167	0.1144
Network efficiency decrease rate	0.00%	***-2.86%***	-1.75%	-2.30%	-1.75%	-1.83%	-2.86%	-4.52%	-6.43%	-7.38%	***-9.21%***
Malicious attack nodes	Original network	71	56	72	96	67	49	68	86	71	69
Network efficiency	0.1260	0.0978	0.1198	0.1101	0.1172	0.0966	0.1157	0.1007	0.1167	0.0978	0.1028
Network efficiency decrease rate	0.00%	-22.38%	-4.92%	-12.62%	-6.98%	***-23.33%***	-8.17%	-20.08%	-7.38%	-22.38%	-18.41%

As shown in Table 3, after the independent random attack, the highest decrease rate of the network efficiency is 2.86% (from 0.1260 to 0.1224), while after the continuous attack, the highest decrease rate of the continuous attack is 9.21% (from 0.1260 to 0.1144). For the malicious attack, the decrease rates of the network efficiency ranges from 4.92% to 23.33%, and 60% of the decreases are more than 10.00%.

It can be concluded that the SMRT network presents high robustness for random attacks. Among the five random attack nodes, the three nodes (94 (Telok Blangah), 61 (Clarke Quay), and 128 (Segar)) are independent nodes, and the nodes 62 (Little India) and 95 (Bayfront) are transfer stations and connect to two rail lines each. For the independent random attack, all the network efficiency decrease rates are below 3%, which demonstrates the high robustness of the network for independent random attacks. As for the continuous attack, the network efficiencies decrease continuously, while the attack nodes increase. When there are five attack nodes, the network efficiency decrease rates reach their largest extent, which is 9.21%.

Comparatively, the malicious attack presents more impacts on the network efficiency. The network efficiency decrease rate for the independent node 67 (Serangoon) is as much as 23.33%, which is the largest decrease after the malicious attack. In Figure 4, the node 67 (Serangoon) is highlighted with a red circle. The Serangoon station is located in northeast Singapore and is one of the transfer stations of the Purple Line and Yellow Line. Due to the special location of the nodes in the network, the attack of this station separates the nodes in the Sengkang LRT and the Punggol LRT as well as five nodes in the Purple Line from the main network, which means that the whole network has been separated into two parts. Under this condition, the trains in the main network cannot reach the separated nodes, and vice versa. Thus, the separation of the network heavily decreases the network efficient.

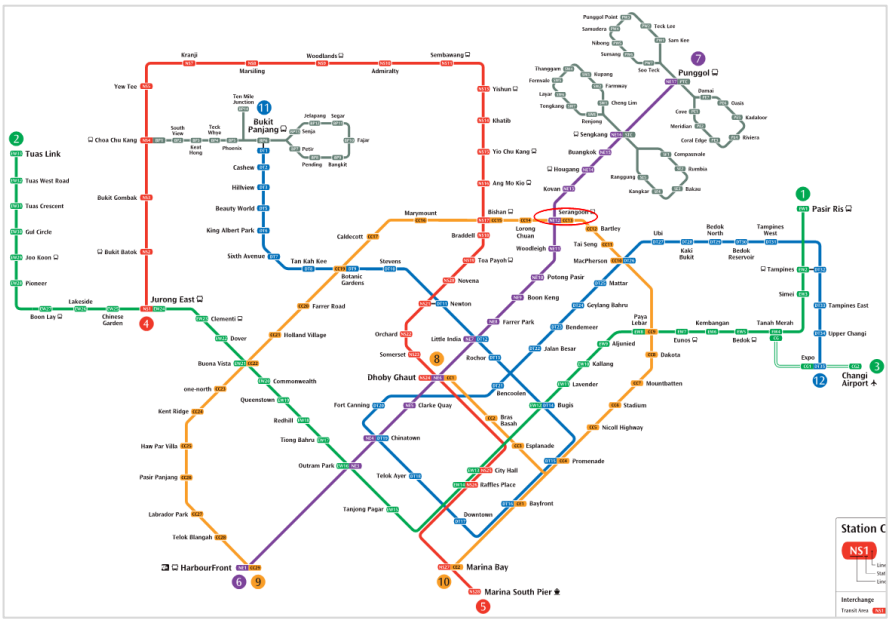

Figure 4. Highlighting the Serangoon station in the SMRT system map

The attack of the nodes 71 (Sengkang), 68 (Kovan), 69 (Hougang), 72 (Punggol), and 96 (Bukit Panjang) could also separate the whole network into two parts or more. Similar to the node 67 (Serangoon), the attack of the nodes 71 (Sengkang), 68 (Kovan), and 69 (Hougang) separates the nodes in the Sengkang LRT and the Punggol LRT from the whole network. The attack of the node 72 (Punggol) separates the nodes in the Punggol LRT from the main network. In addition, the attack of the node 96 (Bukit Panjang) separates seven nodes in the Bukit Panjang LRT from the main network. The above attacks lead to a significant decrease in network efficiencies. Moreover, the attack of the nodes 49 (Bishan), 86 (Botanic Gardens), and 56 (Dhoby Ghaut) also leads to an obvious decrease in network efficiencies. The three nodes are important transfer nodes in the network, especially node 56 (Dhoby Ghaut), which is the connection of three lines (Purple Line, Red Line, and Yellow Line). Thus, the nodes in special locations, such as the nodes that link to different sections of the network, connect a cluster of nodes to the main network, or connect to more than one rail transit line, are all the important nodes in the network. It can be concluded that the malicious attack of important nodes would significantly impact the robustness of the network.

5.1.2. Horizontal Analysis for the Network Connectivity

The connectivity of the original network is 0.01454. The decreases in connectivity after the random attack and malicious attack are shown in Table 4.

Table 4. The connectivity decrease and decrease rates after the two types of attacks

Random attack nodes	Original network	62	94	61	128	95	62	62→94	62→94→61	62→94→61→128	62→94→61→128→95
Connectivity	0.01451	0.01419	0.01435	0.01435	0.01435	0.01427	0.01427	0.01411	0.01395	0.01379	0.01355
Connectivity decrease rate	0.00%	-2.21%	-1.10%	-1.10%	-1.10%	-1.65%	-1.65%	-2.76%	-3.86%	-4.96%	-6.62%
Malicious attack nodes	Original network	71	56	72	96	67	49	68	86	71	69
Connectivity	0.01451	0.01403	0.01411	0.01411	0.01411	0.01419	0.01419	0.01435	0.01419	0.01403	0.01435
Connectivity decrease rate	0.00%	-3.31%	-2.76%	-2.76%	-2.76%	-2.21%	-2.21%	-1.10%	-2.21%	-3.31%	-1.10%

Table 4 shows that for the independent node attack, the malicious attack presents more influences on network connectivity than the random attack. The calculation of connectivity focuses on the number of true edges of the network. The nodes in the malicious attack have high degree values or betweenness values, and they connect to more edges than other nodes. For example, the nodes 71 (Sengkang), 56 (Dhoby Ghaut), 72 (Punggol), and 96 (Bukit Panjang) are all transfer stations for two lines or more and connect to five edges or more. Thus, the attacks of the nodes decrease the connections of these edges. Comparatively, in the random attack, the selected five nodes connect two edges, three edges, or four edges. Therefore, the independent malicious attack affects the network connectivity more than the independent random attack. In the continuous random attack, the network connectivity decreases continuously while the isolated nodes increase. After continuous attack by five nodes (62→94→61→128→95), the decrease rate of the network connectivity reaches its maximum of 6.62%.

5.1.3. Horizontal Analysis for the Relative Size of the Maximal Connected Subgraph (*RSMCS*)

Table 5 shows that the random attack has little impact on the parameter RSMCS. RSMCS focuses on the number of nodes in the maximal connected subgraph. After the random attack of the five nodes (62 (Little India), 94 (Telok Blangah), 61 (Clarke Quay), 128 (Segar), and 95 (Bayfront)), including the independent attack and the continuous attack, the attacked nodes become the isolated nodes and the rest of the nodes in the network still connect to each other. Therefore, the RSMCS after the random attack presents less variation. Comparatively, the malicious attack of the nodes 71 (Sengkang), 72 (Punggol), 96 (Bukit Panjang), 67 (Serangoon), 68 (Kovan), and 69 (Hougang) has a clear impact on the parameter RSMCS, which ranges from 79.11% to 94.94%. The illustration of the RSMCS decreases is similar to the illustration of the network efficiency decreases in Section 5.1.1. The above six nodes in the important location of the network are the necessary nodes that link to different sections of the network or connect a cluster of nodes with the main network. The attack of these nodes will separate the network into several sections, which will significantly influence the scale of the subgraph. For example, the attack of 71 (Sengkang station) separates nodes in the Sengkang LRT and the Punggol LRT, as well as two nodes in the Purple Line, from the whole network. Therefore, the maximal connected subgraph in the network is the rest of the network, excluding the separated nodes. The separation of the network decreases the RSMCS obviously. Malicious attacks of the nodes with important locations will significantly impact the robustness of the network.

Table 5. The RSMCS after the two types of attacks

Random attack nodes	Original network	62	94	61	128	95	62	62→94	62→94 →61	62→94→ 61→128	62→94→61 →128→95
RSMCS	100.00%	99.37%	99.37%	99.37%	99.37%	99.37%	99.37%	98.73%	98.10%	97.47%	96.84%
Malicious attack nodes	Original network	71	56	72	96	67	49	68	86	71	69
RSMCS	100.00%	81.65%	99.37%	90.51%	94.94%	79.11%	99.37%	79.75%	99.37%	81.65%	80.38%

5.2. Longitudinal Analysis

The longitudinal analysis was conducted for the three parameters' calculation results in the random attack and malicious attack.

Tables 3-5 show no significant decrease in the three parameters (network efficiency, connectivity, and RSMCS) after the random attack, including the independent attack and continuous attack. Comparatively, the malicious attack of the network presents clear influence in some scenarios, especially after the attack of the important nodes in the network. The important nodes include the nodes linking to different sections of the network, connecting a cluster of nodes with the main network, or connecting to more than one rail transit line. The attack of the important nodes in the network would lead to a decrease in both network efficiency and RSMCS. In the SMRT, the nodes 71 (Sengkang), 72 (Punggol), 96 (Bukit Panjang), 67 (Serangoon), 68 (Kovan), and 69 (Hougang) are important nodes in the network and present high degree values and betweenness values. The attack of these nodes cause the separation of a cluster of nodes from the main network. For example, the attack of the node 67 (Serangoon) would lead to the separation of the nodes in the Sengkang LRT and the Punggol LRT and five nodes in the Purple Line from the whole network, which would significantly influence the network efficiency and the RSMCS. The parameter connectivity focuses on the number of true edges of the network. The attack of some nodes could simply decrease the edges of the network in limited numbers. Thus, compared to network efficiency and RSMCS, the parameter connectivity presents a less obvious decrease. However, the connectivity of the network after the malicious attack still shows more variation than the random attack for independent attacks.

6. Conclusions

As a main kind of public transportation, the urban rail transit has developed rapidly in recent years. Its safety operation should be guaranteed. This paper focused on the exploration of the robustness of the urban rail transit network (URTN). Due to the topological characteristics of the rail transit network, the complex network theory was adopted in this study. The robustness analysis includes the calculation for the topological parameters, the robustness analysis parameters of the URTN, and the establishment of the attack strategies for the URTN. The Singapore Mass Rapid Transit System (SMRT) was used for the case study, and the proposed methodology was implemented. The results were discussed from horizontal and longitudinal angles. The results could be summarized as follows:

- The malicious attack has more serious impacts on the URTN than the random attack, especially reflected by the robustness assessment parameters network efficiency and relative size of the maximal connected subgraph (RSMCS).
- The decrease in the robustness is caused by the attack of some important nodes, which are the nodes linking to different sections of the network or connecting a cluster of nodes to the main network. This means that if these kinds of nodes are attacked, the network would be separated into several sections and decrease the robustness of

the network to a large degree. Therefore, the results suggest that the protection of these kinds of nodes should be strengthened.

- The attacks of the transfer stations show more influence on the network robustness than the nodes in one rail transit line. Thus, the safety of the transfer stations for multi rail transit lines should also be paid more attention.

This research shows the meaningful aspects in methodology and results. The obtained results could supply useful references for the practical management of URTN, and the proposed methodology could be applied to other UTRN robustness analyses.

Acknowledgements

This work was supported by research funds from the National Natural Science Foundation of China (No. 71801026), MOE (Ministry of Education in China) Project of Humanities and Social Sciences (No. 17YJC630189), and Chongqing Research Program of Basic Research and Frontier Technology (No. cstc2017jcyjAX0359).

References

1. L. Sun, Y. Huang, Y. Chen, and L. Yao, "Vulnerability Assessment of Urban Rail Transit based on Multi-Static Weighted Method in Beijing , China," *Transportation Research Part A*, Vol. 108, pp. 12-24, 2018
2. Y. Yang, Y. Liu, M. Zhou, F. Li, and C. Sun, "Robustness Assessment of Urban Rail Transit based on Complex Network Theory: A Case Study of the Beijing Subway," *Safety Science*, Vol. 79, pp. 149-162, 2015
3. H. Xu, L. Jiao, S. Chen, M. Deng, and N. Shen, "An Innovative Approach to Determining High-Risk Nodes in a Complex Urban Rail Yransit Station : A Perspective of Promoting Urban Sustainability," *Sustainability*, Vol. 10, No. 7, pp. 2456, 2018
4. H. Kim, C. Kim, and Y. Chun, "Network Reliability and Resilience of Rapid Transit Systems," *The Professional Geographer*, Vol. 68, No. 1, pp. 53-65, 2016
5. E. Rodr ́guez-N úñez and J. C. Garc á-Palomares, "Measuring the Vulnerability of Public Transport Networks," *Journal of Transport Geography*, Vol. 35, pp. 50-63, 2014
6. X. Wang, Y. Ko ç, S. Derrible, S. N. Ahmad, W. J. A. Pino, and R. E. Kooij, "Multi-Criteria Robustness Analysis of Metro Networks," *Physica A*: *Statistical Mechanics and Its Applications*, Vol. 474, pp. 19-31, 2017
7. M. Kyriakidis, R. Hirsch, and A. Majumdar, "Metro Railway Safety: An Analysis of Accident Precursors," *Safety Science*, Vol. 50, No. 7, pp. 1535-1548, 2012
8. S. Derrible and C. Kennedy, "The Complexity and Robustness of Metro Networks," *Physica A*: *Statistical Mechanics and Its Applications*, Vol. 389, No. 17, pp. 3678-3691, 2010
9. J. Zhang, M. Zhao, H. Liu, and X. Xu, "Networked Characteristics of the Urban Rail Transit Networks," *Physica A*, Vol. 392, No. 6, pp. 1538-1546, 2013
10. Z. Zhou, J. Irizarry, and Q. Li, "Using Network Theory to Explore the Complexit of Subway Construction Accident Network (SCAN) for Promoting Safety Management," *Safety Science*, Vol. 64, pp. 127-136, 2014
11. P. Angeloudis and D. Fisk, "Large Subway Systems as Complex Networks," *Physica A*: *Statistical Mechanics and Its Applications*, Vol. 367, pp. 553-558, 2006
12. Y. Yang, Y. Liu, M. Zhou, F. Li, and C. Sun, "Robustness Assessment of Urban Rail Transit based on Complex Network Theory: A Case Study of the Beijing Subway," *Safety Science*, Vol. 79, pp. 149-162, 2015
13. H. Kim and Y. Song, "An Integrated Measure of Accessibility and Reliability of Mass Transit Systems," *Transportation*, Vol. 45, No. 4, pp. 1075-1100, 2018
14. J. Zhang, X. Xu, L. Hong, S. Wang, and Q. Fei, "Networked Analysis of the Shanghai Subway Network , in China Networked Analysis of the Shanghai Subway Network , in China," *Physica A*, Vol. 390, No. 23-24, pp. 4562-4570, 2011
15. D. J. Sun, Y. Zhao, and Q. Lu, "Vulnerability Analysis of Urban Rail Transit Networks: A Case Study of Shanghai, China," *Sustainability*, Vol. 7, pp. 6919-6936, 2015
16. Q. Lu, "Modeling Network Resilience of Rail Transit under Operational Incidents," *Transportation Research Part A*, Vol. 117, No. March, pp. 227-237, 2018
17. D. Jian and S. Guan, "Measuring Vulnerability of Urban Metro Network from Line Operation Perspective," *Transportation Research Part A*, Vol. 94, No. 800, pp. 348-359, 2016
18. J. Zhang, S. Wang, and X. Wang, "Comparison Analysis on Vulnerability of Metro Networks based on Complex Network," *Physica A*: *Statistical Mechanics and Its Applications*, Vol. 496, pp. 72-78, 2018
19. A. A. Barabási, R. Albert, and A. C. S. T. O. Lsmo, "Emergence of Scaling in Random Networks," *Science*, Vol. 286, pp. 509-512, 1999
20. H. Xu, J. Zhang, J. Yang, and L. Lun, "Node Importance Ranking of Complex Network based on Degree and Network Density," *International Journal of Performability Engineering*, Vol. 15, No. 3, pp. 850-860, 2019
21. C. Von Ferber, T. Holovatch, Y. Holovatch, and V. Palchykov, "Public Transport Networks: Empirical Analysis and Modeling," *European Physical Journal B*, Vol. 68, No. 2, pp. 261-275, 2009
22. S. H. Strogatz, "Exploring Complex Networks," *Nature*, Vol. 410, pp. 268-276, 2001
23. SMRT Train Ltd., "SMRT Train Ltd. Operations Review 2017," Singapore, 2017