

Vulnerability Assessment of Metro Systems Based on Dynamic Network Structure

Jun Pu^{1,2}, Chuanren Liu³, Jianghua Zhao^{1,2}, Ke Han⁴, and Yuanchun Zhou¹

¹ Computer Network Information Center,
Chinese Academy of Sciences, Beijing, China
`{pujun, zjh, zyc}@cnic.cn`

² University of Chinese Academy of Sciences, Beijing, China

³ Decision Sciences and Management Information Systems,
Drexel University
`chuanren.liu@drexel.edu`

⁴ Department of Civil and Environmental Engineering,
Imperial College London, United Kingdom
`k.han@imperial.ac.uk`

Abstract. Invulnerable metro systems are essential for the safety and efficiency of urban transportation services. Therefore, it is of significant interest to systematically assess the vulnerability of metro systems. To this end, in this paper, we assess the vulnerability of metro systems with a data-driven framework in which dynamic travel patterns are considered. Specifically, we use effective attack strategies based on the topology structure of metro networks. The network structure depends on not only connectivity among metro stations but also dynamic passenger flow patterns. Thus, two data-driven metrics, satisfaction rate (SR) and satisfaction rate with path cost (SRPC), are proposed to quantify the vulnerability of metro networks after our attack strategies. Finally, we conduct experiments on Shanghai metro system. The results indicate that the metro system is vulnerable to malicious attacks while it shows strong robustness to random failures. Our results also highlight weak-points and bottlenecks in the system, which may bear practical managerial implications for policymakers to improve the reliability and robustness of the metro system and the public transportation services.

Keywords: Metro systems, Network vulnerability, Node centrality, Travel patterns, Dynamic networks

1 Introduction

With the rapid development of the economy, public infrastructure such as metro system has played an essential role in public transportation services for large cities. Due to the severe and ever-increasing traffic pressure in the metropolis, more and more passengers consider the public transportation services especially the metro system as their primary choice for short-distance travels. For instance,

the daily ridership of Shanghai metro system is about 10 million on average, and the annual ridership was 3.4 billion in 2016⁵.

Developing at such a rapid pace, metro systems are facing new challenges and requirements on providing secure, reliable, and sustainable services. A number of attacks at city metro systems have occurred in the past few years around the world. Therefore, analyzing the vulnerability of metro systems will help policymakers and urban administrators to develop and operate metro systems in a well-informed way. In particular, the vulnerability analysis for a city metro network provides us with a better understanding of the robustness of the system in the case of unexpected events.

In this paper, we develop a data-driven framework to assess the vulnerability of metro systems based on dynamic topology structure of metro networks. To be specific, we construct the metro network and measure the vulnerability of the network under different ridership distributions. We develop the framework on the basis of various attack strategies and spectral analysis of network centrality. Particularly, we develop a weighted subgraph centrality method to incorporate dynamic passenger flow patterns. Further, we propose two data-driven metrics based on dynamic ridership data to quantify the vulnerability and the transportation efficiency of metro systems. With our framework, we can analyze the vulnerability of metro systems not only from the static topology perspective but also by incorporating dynamic travel patterns.

In the empirical study, we use Shanghai metro system and the daily ridership data to evaluate our framework. The Shanghai metro system, established in 1993, is now the world's largest urban metro traffic system measured by route length. Up to present, Shanghai urban metro system consists of 14 lines (not including magnetic lines) and covers 13 municipal districts with the total route length of 617 kilometers. Our results indicate that the metro system is vulnerable to malicious attacks while it shows strong robustness to random failures. A detailed analysis based on our results provides policymakers and urban administrators with practical managerial implications to improve the reliability and robustness of the metro system and the public transportation services.

The rest of our paper is organized as follows. Section 2 introduces related works about vulnerability assessment mainly from the view of topology structures of metro networks. Section 3 describes our framework with three parts: attack strategies, subgraph centrality, and vulnerability metrics. Finally, we present experimental results in Section 4 and conclude our work in Section 5.

2 Related Work

Network vulnerability has been the focus of research in various fields [1–4, 6–10, 16]. As one of the pioneering studies on network vulnerability, Albert and Barabási [1] studied the robustness of two real networks under malicious attacks and random failures, and showed that the scale-free networks were more vulnerable under intentional attacks. Holme [7] et al. adopted four different attack

⁵ <http://www.shmetro.com/>

strategies based on network betweenness to evaluate the vulnerability of the Internet and interpersonal relationship networks. As the transportations around us can be easily modeled with networks, many scientists introduced the vulnerability concept into the transportation field. Jenelius and Mattsson [9] analyzed the road network vulnerability and argued that an event which happened locally may spread on the network thus lead to serious disasters. Berche et al. [2] used two ways to construct the transportation networks, and then studied the resilience of public transportation networks by simulating different attack strategies. Derrible [3] looked at 33 metro systems and used theoretical network methods to analyze the robustness of metro systems. Jenelius and Cats [8] evaluated the network robustness with the consideration of passenger welfare under disruptions after adding new links to networks.

Those studies mentioned above mostly analyzed network vulnerability from the static view of network topology. However, transportation network structures often change with dynamic ridership distributions and passenger travel patterns. A network with different ridership distributions may bear different vulnerabilities and inefficiencies when faced with unexpected changes in the network topology. Therefore, in this paper, we study the problem of vulnerability assessment for transportation systems based on dynamic network structure.

3 Vulnerability Assessment Framework

One straightforward and effective approach to vulnerability assessment of a network system is to conduct a variety of attacks and measure the attack impacts on the network system. Obviously, implementing this approach in real-world is often too costly to be feasible. For example, disrupting the metro networks in cities could lead to social and economic losses of a large population. Therefore, in this paper, we develop a data-driven framework to simulate both random and malicious attacks on the network system, then estimate the attack impacts using vulnerability metrics.

3.1 Attack Strategies

The attack strategies basically fall into two types: random failure and malicious attack [12, 18]. These two kinds of attacks are carried out by removing the nodes (e.g., metro stations) and all the edges linked to the nodes. The malicious attack aims at destroying the most important nodes so as to paralyze the functionality of the whole network (e.g., a metro system) to the greatest extent [11, 15, 17]. The random failure is specified as the dysfunction which results from the failure on some nodes with a random probability [15]. In this work, we adopt these two strategies to randomly and intentionally paralyze (remove) network nodes respectively. For malicious attack, we target a set of important nodes, where the importance of each node is measured by subgraph centrality [5]. Particularly, we develop the weighted subgraph centrality by incorporating dynamic ridership distributions.

3.2 Subgraph Centrality

Prior to malicious attacks, a crucial step is to measure the centrality of each station and identify the hubs. Several measurements, such as degree and betweenness, are usually adopted in many studies [2, 15]. However, Yan et al. [14] argued that the measurement based on spectral method is a better indicator for network analysis, as it contains abundant characteristics of networks [13]. Therefore, in our study, we adopt a spectral method – subgraph centrality [5] to calculate the importance of each station.

The subgraph centrality is an improvement of degree centrality, and it better explains the centrality from the view of the topology of a network. It determines the importance of each node on the basis of its participation to the local subgraphs. Specifically, it is defined as the sum of closed walks that start and end at a certain node. Each closed walk represents a connected subgraph of the network, and a weight is assigned to it as smaller subgraph gets a higher weight. Thus, the centrality of a node can be measured by counting the sum of the different subgraphs that the node participates in, and smaller subgraph adds more importance to the node. The subgraph centrality is defined as follows:

$$SC(i) = \sum_{k=0}^{\infty} \frac{\mu_k(i)}{k!} \quad (1)$$

$$\mu_k(i) = (A^k)_{ii} \quad (2)$$

where $\mu_k(i)$ denotes the number of closed walks that start and end at node i through k steps. To avoid the case that $\sum_{k=0}^{\infty} \mu_k(i)$ diverges, it is divided by the factorial of length k . $(A^k)_{ii}$ is the i -th diagonal element of the k -th power of adjacency matrix A of a network.

Lemma 1. *Given an undirected network $G(V, E)$, where V is the set of N nodes and E denotes L edges. The upper bound of the subgraph centrality for each node i in V is:*

$$\lceil SC(i) \rceil = e^{\lambda_{main}}$$

where λ_{main} is the main eigenvalue of adjacency matrix A of network G .

Proof. The network G is an undirected graph and thus adjacency matrix A is a symmetric matrix. Therefore, the eigen decomposition for A can be written as: $A = QAQ^T$, where Q is an orthogonal matrix (the orthonormal basis) with real and normalized eigenvectors $q_1, q_2, \dots, q_N$ of A . The corresponding eigenvalues are $\lambda_1, \lambda_2, \dots, \lambda_N$ and the diagonal matrix is written as $\Lambda = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_N)$. Thus we can obtain $A^k = QA^kQ$ and $\Lambda^k = \text{diag}(\lambda_1^k, \lambda_2^k, \dots, \lambda_N^k)$, so $(A^k)_{ii} = \|q_i\|_2^2 \lambda_i^k$. As q_i is an orthogonal and normalized real eigenvector, we can obtain $\|q_i\|_2^2 = 1$ and $(A^k)_{ii} = \lambda_i^k$ thus $SC(i) = \sum_{k=0}^{\infty} \frac{(A^k)_{ii}}{k!} = \sum_{k=0}^{\infty} \frac{\lambda_i^k}{k!}$. Based on Maclaurin series, it turns to: $\sum_{k=0}^{\infty} \frac{\lambda_i^k}{k!} = e^{\lambda_i}$. Thus we arrive at $SC(i) = e^{\lambda_i} \leq e^{\lambda_{main}}$.

Mathematically, the subgraph centrality can be calculated from the spectra of the adjacency matrix of the network, as shown in Theorem 1.

Theorem 1. *Let R^N be the space generated by the eigenvectors of the adjacency matrix A , and $(q_1, q_2, \dots, q_N)$ be the orthonormal basis of space R^N . q_j denotes an eigenvector corresponding to the eigenvalue λ_j and $q_j(i)$ is the i -th element in q_j . Thus, the subgraph centrality $SC(i)$ can be obtained by:*

$$SC(i) = \sum_{j=1}^N [q_j(i)]^2 e^{\lambda_j} \quad (3)$$

Furthermore, in this paper, we not only measure the centrality based on static network topology, but also propose a weighted measurement by incorporating the ridership distribution. That is, the dynamic ridership matrix W is considered in the measurement instead of the adjacency matrix A . Thus, we modify SC to a weighted one – WSC, which is described as follows:

$$WSC(i) = \sum_{j=1}^N [q_{wj}(i)]^2 e^{\lambda_{wj}} \quad (4)$$

where $(q_{w1}, q_{w2}, \dots, q_{wN})$ are the eigenvectors corresponding to the eigenvalues $(\lambda_{w1}, \lambda_{w2}, \dots, \lambda_{wN})$ of the normalized weight matrix $\widetilde{W}$, which is obtained by normalizing the original ridership matrix W using min-max scaling:

$$\widetilde{W}_{i,j} = \frac{W_{i,j} - \min(W)}{\max(W) - \min(W)} \quad (5)$$

where element $W_{i,j}$ means the number of passengers who have to go through the edge between stations i and j to achieve their destinations.

3.3 Vulnerability Metrics

The attacks (i.e., the removal of stations) will usually have a significant impact on the metro system operation. Thus, we define vulnerability metrics by quantifying such an impact on the vulnerability of the metro network. Specifically, we use the real ridership data to define the evaluation metrics. To this end, we assume that all passengers choose the shortest paths as their travel paths from the start stations to the destination stations. After the attacks, the passengers will cancel their travels by metro if: (i) the length of the new travel path is n stations more than the path before; or (ii) there is no way to connect the source and destination stations.

On the basis of the assumptions, we can estimate the number of travels (ridership) which are not influenced by the attacks, as defined by satisfaction rate (SR):

$$SR = \frac{M - C}{M} = \frac{\sum_{i,j \in G', i \neq j} I(i,j) \times r_{i,j}}{\sum_{i,j \in G, i \neq j} r_{i,j}}, \quad (6)$$

where

$$I(i, j) = \begin{cases} 0 & \text{if } l'(i, j) - l(i, j) > n \\ 1 & \text{otherwise} \end{cases}. \quad (7)$$

Note that, M is the total ridership and C is the sum of cancelled travels. G and G' are connected graphs of the original metro network and the network after attacks, respectively. $r_{i,j}$ is the number of ridership that gets on at i and gets off at j . $l(i, j)$ measures the length of shortest path between i and j in G . According, $l'(i, j)$ is the shortest path length calculated in the network G' after attacks. In other words, $I(i, j)$ is the indicator function that indicates whether the new path length between station i and j is n or above longer than that before attacks.

The satisfaction rate (SR) effectively quantify the changes in ridership due to the attacks on the metro network. However, different ridership often bears different travel cost, as measured by the length or the number of stations travelled by the passengers. To incorporate the travel cost in evaluating the network vulnerability, we define the satisfaction rate with path cost (SRPC), which combines the length of the shortest path and the ridership on the same path:

$$SRPC = \frac{\sum_{i,j \in G', i \neq j} I(i, j) \times r_{i,j} \times l'(i, j)}{\sum_{i,j \in G, i \neq j} r_{i,j} \times l(i, j)} \quad (8)$$

Both SR and SRPC can be regarded as the efficiency of the metro system, as they estimate to which level the metro system can satisfy the demand of all passengers with efficient transportation services.

4 Experimental Analysis and Discussion

4.1 Data Preprocessing

In 2016, Shanghai Government Data Service Website⁶ released several types of public transportation data, including the transaction data of public transportation cards generated in April 2015. The sensitive personal information has been kicked out in the transaction, and it mainly records the elements as: $\{card\ ID, date, time, station, amount\ and\ type\ of\ transportation\}$. According to this data, we first extract the transactions made on the metro system. As a cardholder only have to swipe the card when getting in and getting out of the metro system, we tease out the travel routes based on the records of stations over time for every cardholder. So each pair of stations ordered by time is regarded as one travel and the shortest path between them is the travel route. Thus the ridership on one travel route can be easily obtained by summing up the same pairs of source and destination stations from different cardholders. The map of Shanghai metro network operated in 2015 can be referenced from the website of Shanghai Metro⁷.

⁶ <http://www.datashanghai.gov.cn/>

⁷ <http://service.shmetro.com/en/>

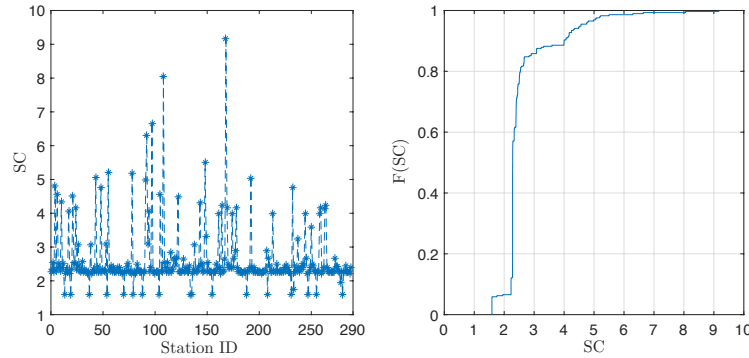


Fig. 1. The left panel shows the subgraph centrality (SC) for each numbered station, and the right one shows the cumulative distribution function (CDF) of SC values.

4.2 Topological Properties of Metro Network

To give an overall understanding of Shanghai metro, some basic topological characteristics of the network are concluded. Firstly, the metro network is constructed as an undirected graph, in which the nodes represent the stations and the links mean that the two connected stations are neighbors. Then we calculate the characteristics, and there are 289 stations and 322 edges within the network. The diameter (the longest shortest path) of the network is 42. The average shortest distance $\langle l \rangle$ is 15.294 and the average degree $\langle k \rangle$ is 2.228, which means most of the stations are normal stations.

Prior to malicious attack simulations, we use the subgraph centrality (SC) to evaluate the importance of each station based on the network topology. The SC results and the cumulative distribution function (CDF) are shown in Fig. 1.

The left figure in Fig. 1 shows the SC values for the stations, and the values of most stations are concentrated in 2.0–2.5. The CDF indicates that nearly 90% stations are with an SC value lower than 4. Afterwards, we pick up the top-10 important stations as the targets of malicious attack. These stations are *Century Ave.* (SC=9.166), *Xujiahui* (SC=8.052), *People's Square* (SC=6.642), *Shanghai Indoor Stadium* (SC=6.291), *Yishan Rd.* (SC=5.499), *Longde Rd.* (SC=5.218), *Jinshajiang Rd.* (SC=5.181), *Caoyang Rd.* (SC=5.069), *Oriental Sports Center* (SC=5.038) and *Longyang Rd* (SC=4.978). Figure 2 depicts the locations of these important stations with red circles. As can be seen from Fig. 2, these stations are located in every direction of the city and they are indeed the important transfer stations in reality. Besides, these stations are all on the edge of downtown areas and serving as the connecting stations between suburban and downtown.

4.3 Vulnerability Analysis and Travel Patterns

Since most lines of Shanghai metro open at 5:30 and close at 23:30, we aggregate the ridership within every three hours from 3:00 to 24:00 for each day. Thus there are 7 aggregated periods on each day and totally 210 periods in April.



Fig. 2. The top-10 influential stations of Shanghai metro system.

The ridership (upper panel in Fig. 3) presents a periodic pattern over time, with rush commuting hours from 6:00 to 9:00 and from 18:00 to 21:00 on every day. However, during the weekends and holidays (April 6th is the Tomb-sweeping Festival of China), the ridership has fallen by half and the rush hours turn to the period from 12:00 to 15:00. To analyze the vulnerability of each time period, we simulate the two attack strategies as described before on the metro system. Firstly, we suppose that the travel will be cancelled if the new shortest path is $n = 5$ (or above) stations longer than before. SR and SRPC are used to indicate the vulnerability of the metro system after attacks. In malicious attacks, we mainly attack and remove the top ten stations which are measured by subgraph centrality (SC). While in random failures, we randomly remove ten stations to calculate the vulnerability metric values and repeat this for ten times. Thus the results for random failures are averaged from ten simulations. The results are shown in the middle and bottom figures of Fig. 3.

As can be seen from the middle figure of Fig. 3, SR metric indicates that the metro network appears to be extremely vulnerable to the malicious attacks. Only nearly 50% travels can be still carried on the metro, and the delivery efficiency indicated by SRPC is about 40%. However, from the bottom figure in Fig. 3, the metro network shows strong robustness to random failures. SR metric illustrates that about 90% travels can be satisfied after random failures, and SRPC shows that the delivery efficiency of the metro system reaches 80%. Two metrics both indicate that the most robust period is from 21:00 to 24:00 for each day after malicious attacks and random failures. Whereas, the weakest period is the morning rush-hour from 6:00 to 9:00, as this period is always with the lowest vulnerability value.

To better understand the correlation between the absolute amount of ridership and vulnerability, we pick out the ridership data during the period from 6:00 to 9:00 for each day and the corresponding SR and SRPC values. As shown

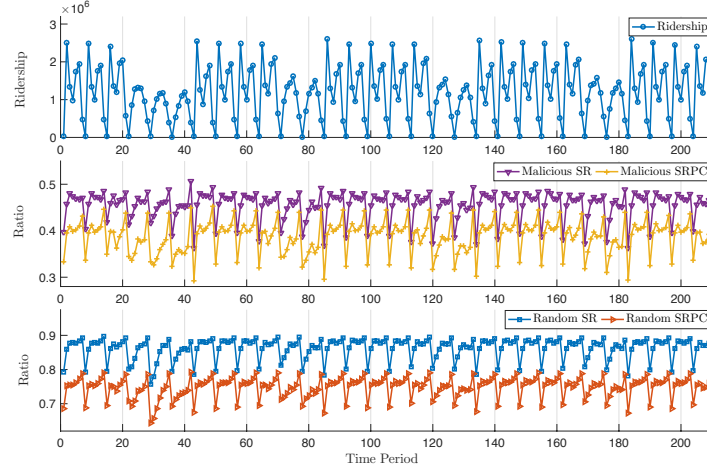


Fig. 3. The top panel shows the ridership aggregated for every three hours from 3:00 to 24:00 of every day in April. The lower two ones show the vulnerability ratios of the metro network after malicious attacks and random failures, respectively.

in Fig. 4(a), SR and SRPC are positively correlated with the ridership after both random failures and malicious attacks.

Besides, the vulnerability results from two metrics exhibit a strong correlation after both random failures and malicious attacks. The reason for this phenomenon can be explained by the definitions of these two metrics. SR mainly considers how many travels are not affected by the attacks, while SRPC focuses on the delivery efficiency of the metro system rather than simply considers the number of the travels. In addition, as can be seen from Fig. 3 and Fig. 4(a), SRPC is always lower than SR after all kinds of attacks. This means the travels with a length shorter than the average make up the majority of the unaffected travels, and the long-distance travels are more likely to be affected and cancelled by attacks. Specifically, to prove this, we further separately aggregate the unaffected travels and cancelled travels after malicious attacks and then calculate the average distance (the number of stations) of these two kinds of travels. Figure 4(b) indicates that the average distance of the cancelled travels is longer than that of the unaffected ones in all periods. Plus, another interesting travel pattern is that the people who travel from 3:00 to 6:00 (actually 5:30 to 6:00) always have relatively longer travel routes.

Due to the dynamic passenger flow, the metro network can be seen as a weighted one and its structure changes over time with the passenger flow. Therefore, the ridership should be considered when measuring the centrality of each station. As can be seen from Fig. 3, the peak of the ridership appears in different periods on rest-days (weekends and holidays) and weekdays. The peaks are always the rush-hours in weekdays, while in rest-days the peaks appear at 12:00

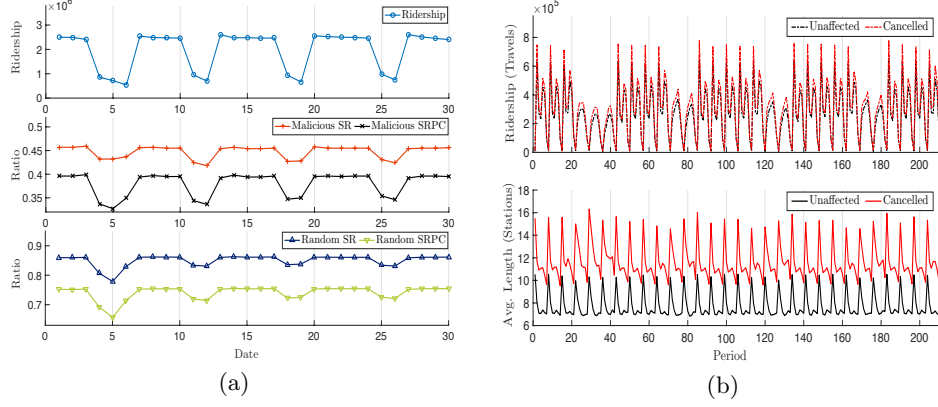


Fig. 4. (a) The correlation between ridership and vulnerability. (b) The upper one shows the number of unaffected and cancelled travels after malicious attacks. The lower one calculates that average distance for these two kinds of travels.

Table 1. The time periods for weekday and rest-day.

Weekday		Rest-day	
Period 1	5:00a.m - 11:00a.m.	Period 5	5:00a.m. - 1:00p.m.
Period 2	11:00a.m - 5:00p.m.	Period 6	1:00p.m. - 8:00p.m.
Period 3	5:00p.m - 8:00p.m.	Period 7	8:00p.m. - 11:00p.m.
Period 4	8:00p.m - 11:00p.m.		

to 15:00. To incorporate these facts, we re-aggregate the travels data to several periods for weekdays and rest-days separately, as shown in Table. 1. This division of the periods is in accordance with our understanding of the daily traffic flow. The Period 1 and Period 3 are the morning and evening rush hours on weekdays. Thus the important stations in these periods may be different from Period 2 and Period 4 when considering the dynamic distribution of passengers.

We firstly calculate the average weight matrices for each of the seven periods based on the travel data of the first 21 days. The fourteen weekdays are used to calculate the average ridership matrices W_1, W_2, W_3 and W_4 for the four periods on weekdays. The seven rest-days (one holiday and three weekends) are used to calculate the matrices W_5, W_6 and W_7 for the three periods in rest-days. Afterwards, we use the proposed weighted subgraph centrality WSC to measure the top-10 stations for each of these seven periods. Last, the malicious attack strategy as described before is simulated on the seven periods of the remaining nine days (including seven weekdays and two rest-days). The results for dynamic malicious attacks are shown in Fig. 5.

As can be seen from it, on weekdays, more than half of the passengers have to cancel their travels on the metro after the dynamic attacks in every period. In

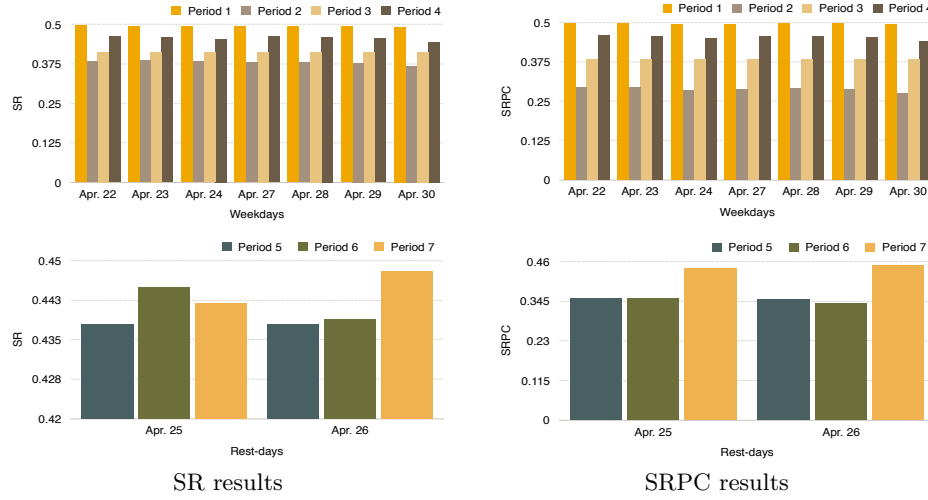


Fig. 5. The SR and SRPC results of dynamic malicious attacks on the last seven weekdays and two rest days in April, 2015.

each weekday, Period 1 seems the most robust period of the whole day. However, according to the SR results on two rest-days, every period presents almost the same vulnerability. But SRPC results show that Period 7 (8:00 p.m. - 11:00 p.m.) has relatively stronger robustness on delivery efficiency when compared with the other two periods in rest-days.

5 Conclusion

We assess the vulnerability of metro system based on the dynamic network structure and travel patterns. Specifically, we develop a framework combining a series of attack strategies and two vulnerability metrics based on dynamic ridership data. By incorporating the ridership, we further develop a weighted subgraph centrality and simulate a dynamic malicious attack strategy. We conduct the empirical study on Shanghai metro system, and the results indicate that the metro system is vulnerable to malicious attacks while it shows strong robustness to random failures. Our results also high-light weak-points and bottlenecks in the system, which may bear practical managerial implications for policymakers to improve the reliability and robustness of the metro system. In the future, we will deploy our vulnerability analysis on more metro systems.

Acknowledgement.

This work is supported by the National Key Research Program of China (No. 2016YFB0501900 and No. 2016YFB1000600). Jun Pu and Chuanren Liu contribute equally to this work. Yuanchun Zhou is the corresponding author.

References

1. Albert, R., Jeong, H., Barabási, A.L.: Error and attack tolerance of complex networks. *Nature* 406(6794), 378–382 (2000)
2. Berche, B., Von Ferber, C., Holovatch, T., Holovatch, Y.: Resilience of public transport networks against attacks. *The European Physical Journal B-Condensed Matter and Complex Systems* 71(1), 125–137 (2009)
3. Derrible, S., Kennedy, C.: The complexity and robustness of metro networks. *Physica A: Statistical Mechanics and its Applications* 389(17), 3678–3691 (2010)
4. Ding, L., Zhang, L., Wu, X., Skibniewski, M.J., Qunzhou, Y.: Safety management in tunnel construction: Case study of wuhan metro construction in china. *Safety Science* 62, 8–15 (2014)
5. Estrada, E., Rodríguez-Velázquez, J.A.: Subgraph centrality in complex networks. *Physical Review E* 71(5), 056103 (2005)
6. Flammini, F., Gaglione, A., Mazzocca, N., Pragliola, C.: Quantitative security risk assessment and management for railway transportation infrastructures. In: *International Workshop on Critical Information Infrastructures Security*. pp. 180–189. Springer (2008)
7. Holme, P., Kim, B.J., Yoon, C.N., Han, S.K.: Attack vulnerability of complex networks. *Physical Review E* 65(5), 056109 (2002)
8. Jenelius, E., Cats, O.: The value of new public transport links for network robustness and redundancy. *Transportmetrica A: Transport Science* 11(9), 819–835 (2015)
9. Jenelius, E., Mattsson, L.G.: Developing a methodology for road network vulnerability analysis. *Nectar Cluster* 1, 1–9 (2006)
10. Lee, K., Jung, W.S., Park, J.S., Choi, M.: Statistical analysis of the metropolitan seoul subway system: Network structure and passenger flows. *Physica A: Statistical Mechanics and its Applications* 387(24), 6231–6234 (2008)
11. Sun, D.J., Guan, S.: Measuring vulnerability of urban metro network from line operation perspective. *Transportation Research Part A: Policy and Practice* 94, 348–359 (2016)
12. Wang, J.: Robustness of complex networks with the local protection strategy against cascading failures. *Safety Science* 53, 219–225 (2013)
13. Watanabe, T., Masuda, N.: Enhancing the spectral gap of networks by node removal. *Physical Review E* 82(4), 046102 (2010)
14. Yan, X., Li, C., Zhang, L., Hu, Y.: A new method optimizing the subgraph centrality of large networks. *Physica A: Statistical Mechanics and its Applications* 444, 373–387 (2016)
15. Yang, Y., Liu, Y., Zhou, M., Li, F., Sun, C.: Robustness assessment of urban rail transit based on complex network theory: A case study of the beijing subway. *Safety Science* 79, 149–162 (2015)
16. Zhang, J., Xu, X., Hong, L., Wang, S., Fei, Q.: Attack vulnerability of self-organizing networks. *Safety Science* 50(3), 443–447 (2012)
17. Zhou, Y., Sheu, J., Wang, J.: Robustness assessment of urban road network with consideration of multiple hazard events. *Risk Analysis* 37(8), 1477–1494 (2017)
18. Zhou, Z., Irizarry, J., Li, Q.: Using network theory to explore the complexity of subway construction accident network (scan) for promoting safety management. *Safety Science* 64, 127–136 (2014)