Creative Construction Conference 2016

Maintenance Strategy of Multi-Equipment Network Systems Based on Topology Vulnerability Analysis

Lieyun Ding, Qi Fang*

School of Civil Engineering & Mechanics, Huazhong University of Science and Technology, Wuhan, P.r. China

Abstract

A great variety of mechanical and electrical equipment are distributed along the whole metro line. Equipment maintenance plays a very important role for metro operation safety. But how to ensure the scientificity and rationality of the maintenance plan remains a problem. Maintenance plan is theoretically supported by existing maintenance strategies. This paper proposes a new maintenance strategy which focuses on multi-equipment network systems based on topology vulnerability analysis. BIM is used as an object-oriented database to store the topological relations of network devices, express the equipment maintenance plan, and form a maintenance information storage and data analysis platform. Then vulnerability analysis of the topological structure is carried out. According to the results of the vulnerability analysis, the maintenance plan of the equipment with high degree of topology vulnerability could be optimized. A case study shows that the optimal maintenance plan based on the proposed maintenance strategy can improve the system reliability and reduce cost.

Keywords: equipment maintenance; BIM; complex network; vulnerability

1. Introduction

In the recent years, with the rapid development of urbanization, the subway transportation has been the one of the main tools to solve the urban traffic problems in China. Shanghai and Beijing subway transportation have entered into the network operation phase. However, the largest number of accident precursors (though not the largest number of injuries) during the metro operation is related to different technical failures (Kyriakidis and Hirsch, 2012) [1]. During the lifetime of subway equipment, degrading will lead to its declining performance. In order to protect the subway safety, the maintenance of the subway equipment plays a very important role [2].

Adopt scientific and reasonable equipment maintenance strategy can improve the reliability of equipment, reduce operation and maintenance costs. Hastak and Baim (2001)[3] analyzed the operation cost of various types of urban infrastructure, and points out that the appropriate maintenance strategy has a great influence on the equipment deterioration degree and maintenance management costs. Some maintenance strategies might offer a cheaper and quicker solution to a problem but might lead to accelerated deterioration and need for higher rehabilitation costs (NCHRP 1979b; Manning and NCHRP 1985, 1988; Shanafelt and NCHRP 1985). Farran (2009) [4] used the Markov Decision Process Model to calculate the infrastructure maintenance costs change according to various maintenance strategies. Through analysis, it is found that, when to take scientific and reasonable maintenance strategy, the equipment has more moderate deterioration curve, longer service life and lower life cycle maintenance cost.

Maintenance strategy itself does not contain specific maintenance objects, combined with the specific working environment (for example Metro Equipment), for each device in the system environment pointed out the applicable service behavior and the condition of its application, the purpose of which is to achieve the maintenance strategy is used to solve the criterion, thereby maintenance plan can be directly applied to the specific system maintenance work. Equipment maintenance plan may contain one or more maintenance strategies to achieve different management objectives (Reliability, Cost rate, Availability et al.).

* Corresponding author. Tel.: +86 18771046116.
E-mail address: fangqi_hust@hotmail.com

Subway equipment maintenance program is mainly divided into 3 parts: 1 maintenance and repair list. The included equipment use the preventive maintenance, not listed equipment default to use the corrective maintenance; 2 maintenance cycle. 3 repair content. Such as visual inspection and functional testing.

Maintenance plan is equipment classification in essence, different maintenance strategies are adopted for different equipment: A device with a high degree of importance need to use the preventive maintenance in shorter maintenance cycle and has more comprehensive maintenance content; the maintenance strategies for devices with low degree of importance is opposite.

At present, The problem of making equipment maintenance plan is how to ensure the rationality of maintenance strategy, that is to say, how to divide the equipment importance more scientifically, to realize the high reliability and low cost.

However, the existing maintenance plan only consider the performance of a single device, and consider the whole system, the subway system can be seen as a complex network system. With the vulnerability of network structure, the vulnerability of each device in the network of the whole equipment will affect its important degree. Therefore, it is necessary to put forward a kind of maintenance strategy based on the vulnerability of the network, more scientific classification of equipment importance, to optimize the equipment maintenance plan.

This paper apply IFC Standard as an object-oriented database, storage the topological relations of network devices and express the equipment maintenance strategy, form a maintenance information storage and data analysis platform, then analyzed the topological structure vulnerability. According to the results of the analysis of the vulnerability, optimize the maintenance strategy of the equipment with high degree of vulnerability.

2. Methodology

2.1. *Complex network theory*

The subway equipment system can be seen as a complex network system which composed of the equipment as the edge, the equipment as the node. The external emergencies such as natural disasters, terrorist attacks and artificial destruction, staff operational errors, equipment failure, may lead to local failure of the line network, thus affecting the normal function of the line of the other part of the equipment, failure will spread to the entire network, leading to more damage, resulting in network capacity and efficiency is reduced obviously. Therefore, subway equipment network has network structural vulnerability, namely in the topology of the network any functional unit reduce or failure, its connected nodes and connections as carrier of communication failure, the failure influence will extend to the local and even the entire network. When due to disturbances or impact a certain point of the subway equipment network failures, that will have a cascading effect, impact on the connectivity of the point line, and the key node failure and even cause network paralysis. Wang Z [5] reviews the methodologies used in vulnerability analysis of transportation networks and particularly focuses on the application of complex network theory.

2.2. *BIM and IFC*

BIM (Building Information Modeling) technology has attracted more and more attention in AEC/FM (Architecture, Engineering and Construction/ Facility Management) field because it introduces a revolutionary technology comparable to CAD that emerged about two decades ago. BIM is an object-oriented database: Faraj et al. developed an IFC Web-based collaborative construction computer environment called WISPER (Web-based IFC Shared Project Environment), which built an IFC-based object-oriented database to help users realize the network integration and sharing of the design, budget, schedule and other information in construction projects[6]. To help facility managers better manage lifecycle information pertinent to managing the facility and responding to facility related patient safety events, an object oriented product model is proposed in the context of developing a healthcare facility information management framework [7]. Thus, this paper apply BIM to storage the topological relations of network devices which is needed in complex network theory and express the equipment maintenance strategy.

3. Basic theory of complex network

Complex network is a network model with a large number of nodes and complex connection topology. In 1998, Watts et al. [8] proposed the concept of the famous small world network. In 1999, Barabbsi et al. [9] proposed the concept of scale free network. Currently, many systems can be viewed as complex networks, such as the Internet, social networks, and rail networks. Complex network theory is used to study the common characteristics of all kinds of complex networks and to deal with them. There are many statistical characteristics to describe the complex network structure, including the shortest path, clustering coefficient, betweenness centrality, average degree and average distance, connectivity distribution, correlation coefficient, of which there are three most basic and important statistical characteristics, namely degree, clustering coefficient and average path length, Here is a brief description of them.

3.1. *Degree and degree distribution of nodes*

The degree i of the node k represents the total number of edges connected to the node i. The average value of the degree k of all nodes in the network is defined as the average degree of the network, which is defined as <k>. Distribution function p(k) express the network node degree distribution, its meaning is the probability of randomly choosing a nodes of k edges, is also equal to the ratio of k degree nodes and the total number of nodes in the network.

3.2. *Network path length*

The shortest path between nodes i and j in the network is defined as the minimum number of sites connected to the two nodes. The average path length L of the network is defined as the value of the average distance between any two nodes, namely

$$L = \frac{1}{\frac{1}{2}N(N+1)} \sum_{i \geq j} d_{ij} \quad (1)$$

In the formula: N is the number of nodes in the network; d_{ij} is the shortest path between the nodes i and j. Here is defined as the minimum number of the site to connect the two nodes.

3.3. *Vulnerability of network structure*

Vulnerability is a sensitive factor that indicate the decrease of service level due to the impact of events. The vulnerability of equipment system can be defined as the probability of the equipment system global efficiency under the attack of different equipment. There are a number of indicators to the network vulnerability, including the relative size of the maximal connected sub graph [10], and network efficiency [11]. The author describes the vulnerability by the equipment network efficiency.

Network efficiency E is used to measure the efficiency of node exchange information in the network. Before G is defined the average network efficiency, the shortest path between any two points $\{d_{ij}\}$ is needed. Set e_{ij} as the efficiency between the vertices i and j which is the reciprocal of the shortest path: $e_{ij} = 1/d_{ij}$, when there are no edge connection between i and j, $d_{ij} = +\infty$, $e_{ij} = 0$, so the average network efficiency of G can be defined as:

$$E(G) = \frac{\Sigma_{i \neq j \in G} e_{ij}}{N(N-1)} = \frac{1}{N(N-1)} \sum_{i \neq j \in G} \frac{1}{d_{ij}} \quad (2)$$

When the value of E is very large, the network efficiency is very high and the connectivity is very good. When node i was attacked, the network is destroyed, network efficiency is also affected, different node failure causes different network efficiency change, so the vulnerability of node i is defined as:

$$\xi_V = \left[E(G_i') / E(G) \right]^{-1} \quad (3)$$

In the formula: G_i' indicates that the node i in G has been attacked and failed, $E(G_i')$ shows the average network efficiency after node i failure, $E(G_i')/E(G)$ is the percentage of the network efficiency and the original efficiency after the failure. Vulnerability ξ_V is expressed as the reciprocal of the efficiency, the greater ξ_V is, the higher vulnerability of the node is, and the network failure caused by node failure is more serious [12]. The biggest vulnerability node is the key nodes that has the highest influence for the overall network efficiency. After defining the network efficiency E, we can determine the key nodes in the network.

4. Case study

4.1. *Network structure of a subway equipment network*

Taking a subway smoke exhaust equipment network as the object of study, analyzing the vulnerability of the topology structure in depth.

First, we extend the IFC framework to apply the attribute set for the vulnerability analysis of metro equipment. Because of the need to establish the complex network model, we need to obtain the relationship between the upstream and downstream of the equipment, and the upstream and downstream of each device will be connected to form a complete network of equipment. Therefore, four attributes of the entity object will extend for APYF, AFHF, Air valve and so on devices, as shown in Figure 1: Ifcfacilityno (the number of equipment in calculation), Ifcfacilitycode (the equipment code in metro facility network), Ifcupstreamfacilitycode (Coding of upstream equipment), Ifcdownstreamfacilitycode (Coding of downstream equipment).

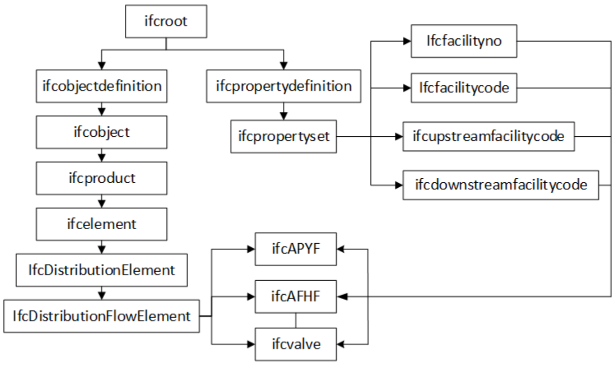

Figure 1 Kernel of the maintenance schema in Express-G format

Facility No.	Facility Code	Facility Type	Upstream facility	Downstream equipment
1	W-E-F03-01-ER04-01-KT_F-4101	Static pressure tank		W-E-F03-01-AR02-01-KT_F-1509
2	W-E-F03-01-AR02-01-KT_F-1509	APYF	W-E-F03-01-ER04-01-KT_F-4101	W-E-F03-01-AR02-01-KT_F-1508
3	W-E-F03-01-AR02-01-KT_F-1508	DT-Electric regulating air valve	W-E-F03-01-AR02-01-KT_F-1509	W-E-F03-01-ER04-01-KT_F-0803
4	W-E-F03-01-ER04-01-KT_F-0803	PY-AS(1)-01	W-E-F03-01-AR02-01-KT_F-1508	W-E-F03-01-AR02-01-KT_F-1528
5	W-E-F03-01-AR02-01-KT_F-1528	APYF	W-E-F03-01-ER04-01-KT_F-0803	W-E-F03-01-ER03-01-KT_F-1501
6	W-E-F03-01-ER03-01-KT_F-1501	Muffler	W-E-F03-01-AR02-01-KT_F-1528	W-E-F03-01-ER03-01-KT_F-1502
7	W-E-F03-01-ER03-01-KT_F-1502	Muffler	W-E-F03-01-ER03-01-KT_F-1501	W-E-F03-01-AR02-01-KT_F-1526
8	W-E-F03-01-AR02-01-KT_F-1526	APYF	W-E-F03-01-ER03-01-KT_F-1502	W-B-F03-01-PS01-01-KT_F-5701/W-B-F03-01-PS01-01-KT_F-5801/W-B-F03-01-PS01-01-KT_F-5901/W-B-F03-01-PS01-01-KT_F-6001/W-B-F03-01-PS01-01-KT_F-5702/W-B-F03-01-PS01-01-KT_F-6101
9	W-B-F03-01-PS01-01-KT_F-5701	Shutter air outlet	W-E-F03-01-AR02-01-KT_F-1526	
10	W-B-F03-01-PS01-01-KT_F-5801	Shutter air outlet	W-E-F03-01-AR02-01-KT_F-1526	
11	W-B-F03-01-PS01-01-KT_F-5901	Shutter air outlet	W-E-F03-01-AR02-01-KT_F-1526	
12	W-B-F03-01-PS01-01-KT_F-6001	Shutter air outlet	W-E-F03-01-AR02-01-KT_F-1526	
13	W-B-F03-01-PS01-01-KT_F-5702	Shutter air outlet	W-E-F03-01-AR02-01-KT_F-1526	
14	W-B-F03-01-PS01-01-KT_F-6101	Shutter air outlet	W-E-F03-01-AR02-01-KT_F-1526	
17	W-E-F03-01-AR02-01-KT_F-1503	APYF		W-E-F03-01-AR02-01-KT_F-1520
18	W-E-F03-01-AR02-01-KT_F-1520	APYF	W-E-F03-01-AR02-01-KT_F-1503	W-E-F03-01-ER04-02-KT_F-4102
19	W-E-F03-01-ER04-02-KT_F-4102	Static pressure tank	W-E-F03-01-AR02-01-KT_F-1520	W-E-F03-01-ER04-02-KT_F-0801

Table 1 the relationship between the upper and lower reaches of a subway exhaust equipment

As shown in the table1, the subway smoke exhaust equipment including muffler, static pressure tank, APYF, AFHF, shutter air outlet, DT-Electric regulating air and so on, totally 99 equipment nodes. Each device has a special code, the code is unique in the entire subway network equipment. Table1 lists the relationship between the upstream and downstream smoke exhaust equipment between all nodes, shows the topology relationship of all equipment in the smoke exhaust system.

4.2. *Vulnerability analysis of Metro Equipment Network*

Using Pajek software establish a directed graph network model of the subway smoke exhaust equipment, and then use the formula (3) to calculate the structure vulnerability of the equipment network.

Calculate the smoke exhaust equipment network number of nodes and the number of edges, average degree, average path length and clustering coefficient. The result is shown in Table2.

Table 2 Characteristic index values of smoke exhaust equipment network

Characteristic index	Value
Number of nodes	99
Number of edges	195
In-degree / Out-Degree / Total-Degree	0.95/0.95/1.90
Average path length	4.46

Table5.2 shows the at present the smoke exhaust system totally has 99 equipment, 195 connected edge, each equipment average directly connect with 1.90 equipment, that indicates the lines cross between less each equipment is not much, and average path length is 446, it has few average path length. According to the complex network theory, the smoke exhaust equipment network has the characteristics of random network.

99 nodes in the network of smoke exhaust equipment were deliberately attacked, and the efficiency of the network was calculated by the formula (2). After calculation, the network efficiency of smoke exhaust equipment network $E(G)$ is 0.0234. After calculation and analysis of the formula (3), shows that the No.9, No.18, No.35, No.46, No.50 nodes have a greater impact on the network efficiency, and the vulnerability coefficient is higher, as shown in Table3.

Table 3 Vulnerability correction factor of partial nodes

Facility No.	Facility Code	Facility Type	$E(G_i')$	Network efficiency change rate/%	ξ_V
9	W-E-F03-01-AR02-01-KT_F-1503	APYF	0.0197	12.34	1.12
18	W-E-F03-01-AR02-01-KT_F-1525	AFHF	0.0205	6.87	1.07
35	W-B-F03-04-ER02-01-KT_F-2087	AFHF	0.0186	16.21	1.16
46	W-B-F03-04-ER02-01-KT_F-2040	AFHF	0.0183	14.13	1.14
50	W-B-F03-04-ER02-01-KT_F-2032	DT-Electric regulating air valve	0.0207	7.92	1.08

4.3. *Maintenance plan optimization*

The result shows that the deliberate attack on a subway exhaust equipment network efficiency is big, the No. 9, No. 35, No.46, are the key nodes with highest vulnerable, should take more stringent equipment maintenance strategy to protect the performance of these devices.

The existing maintenance plan is: do visual inspection for the valves within 6 months. But the No. 9, No. 35, No.46, are the key nodes with highest vulnerable, and higher important degree. We need to optimize their maintenance plan, since the existing original maintenance plan is preventive maintenance, but the maintenance cycle is too long, the maintenance content is too simple. So modify it to do visual inspection and performance testing within 1 month.

5. Conclusion

The author extended the existing IFC standards, applied BIM as an object-oriented database, storage the topological relations of network devices and express the equipment maintenance strategy. And put forward the quantitative analysis method for structure vulnerability of the network, based on complex network theory, from the node degree, the average path length of metro equipment network topology analysis, and proposed the network node vulnerability calculation method based on the network efficiency. The maintenance plan optimization according to the method proposed in this paper, can improve the reliability of the equipment system.

Using complex network theory to analyze the vulnerability of metro equipment network, without taking into account the probability of failure of the station. In the face of natural disasters, the probability of failure of different sites is different, and the vulnerability of the network of metro equipment can be regarded as the integration of the probability of failure and the degree of impact. Subway equipment network vulnerability analysis can take this factor into account, can enrich the subway equipment network vulnerability analysis theory, and the practice has a more important reference.

Acknowledgement

This work was supported in part by a major project of The National Social Science Key Fund of China [grant number 13&ZD175]; The National Natural Science Foundation of China [grant number 71301059].

References:

[1] Kyriakidis, M., R. Hirsch and A. Majumdar, Metro railway safety: An analysis of accident precursors. Safety science, 2012. 50(7): p. 1535-1548.

[2] Marzouk, M. and A. Abdelaty. Maintaining subways infrastructures using BIM. in Proceedings of Construction Research Congress. 2012.

[3] Hastak, M. and E.J. Baim, Risk factors affecting management and maintenance cost of urban infrastructure. Journal of Infrastructure Systems, 2001. 7(2): p. 67-76.

[4] Farran, M. and T. Zayed, Comparative analysis of life-cycle costing for rehabilitating infrastructure systems. Journal of Performance of Constructed Facilities, 2009. 23(5): p. 320-326.

[5] Wang, Z., A.P. Chan and Q. Li. A Critical Review of Vulnerability of Transport Networks: From the Perspective of Complex Network. in Proceedings of the 17th International Symposium on Advancement of Construction Management and Real Estate. 2014: Springer.

[6] Faraj, I., et al., An industry foundation classes Web-based collaborative construction computer environment: WISPER. Automation in Construction, 2000. 10(1): p. 79-99.

[7] Lucas, J., T. Bulbul and W. Thabet, An object-oriented model to support healthcare facility information management. Automation in Construction, 2013. 31: p. 281-291.

[8] Watts, D.J. and S.H. Strogatz, Collective dynamics of 'small-world'networks. nature, 1998. 393(6684): p. 440-442.

[9] Barabási, A. and R. Albert, Emergence of scaling in random networks. science, 1999. 286(5439): p. 509-512.

[10] Albert, R., H. Jeong and A. Barabási, Error and attack tolerance of complex networks. nature, 2000. 406(6794): p. 378-382.

[11] Crucitti, P., et al., Error and attack tolerance of complex networks. Physica A: Statistical Mechanics and its Applications, 2004. 340(1): p. 388-394.

[12] Latora, V. and M. Marchiori, How the science of complex networks can help developing strategies against terrorism. Chaos, solitons & fractals, 2004. 20(1): p. 69-75.