Hindawi
Mathematical Problems in Engineering
Volume 2017, Article ID 8673143, 12 pages
https://doi.org/10.1155/2017/8673143

Research Article

Complexity and Vulnerability Analysis of Critical Infrastructures: A Methodological Approach

Yongliang Deng,[1,2] Liangliang Song,[3] Zhipeng Zhou,[4] and Ping Liu[3,5]

[1]*State Key Laboratory for Geomechanics & Deep Underground Engineering, China University of Mining and Technology, Xuzhou 22116, China*
[2]*School of Mechanics and Civil Engineering, China University of Mining and Technology, Xuzhou 221116, China*
[3]*School of Civil Engineering, Southeast University, Nanjing 210096, China*
[4]*College of Economic and Management, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China*
[5]*School of Civil Engineering, Lanzhou University of Technology, Lanzhou 730050, China*

Correspondence should be addressed to Liangliang Song; 230129183@seu.edu.cn

Received 17 May 2017; Revised 23 August 2017; Accepted 29 August 2017; Published 19 October 2017

Academic Editor: Ruben Specogna

Copyright © 2017 Yongliang Deng et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Vulnerability analysis of network models has been widely adopted to explore the potential impacts of random disturbances, deliberate attacks, and natural disasters. However, almost all these models are based on a fixed topological structure, in which the physical properties of infrastructure components and their interrelationships are not well captured. In this paper, a new research framework is put forward to quantitatively explore and assess the complexity and vulnerability of critical infrastructure systems. Then, a case study is presented to prove the feasibility and validity of the proposed framework. After constructing metro physical network (MPN), *Pajek* is employed to analyze its corresponding topological properties, including degree, betweenness, average path length, network diameter, and clustering coefficient. With a comprehensive understanding of the complexity of MPN, it would be beneficial for metro system to restrain original near-miss or accidents and support decision-making in emergency situations. Moreover, through the analysis of two simulation protocols for system component failure, it is found that the MPN turned to be vulnerable under the condition that the high-degree nodes or high-betweenness edges are attacked. These findings will be conductive to offer recommendations and proposals for robust design, risk-based decision-making, and prioritization of risk reduction investment.

1. Introduction

Social infrastructures are the natural product of infrastructure development at a certain stage, which are the important support and assurance of social development and national economy. For daily activities, modern societies are reliant on dependable functioning critical infrastructure to a large extent, such as electrical supply, water supply, transportation, and communication networks. Critical infrastructures (CIs) can provide various fundamental goods or services for promoting national development and social progress. Furthermore, CIs also play crucial roles in disaster rescue and effective emergency response [1]. For instance, the transportation and telecommunication infrastructures contributed greatly to rescue operations in the Wenchuan deadly earthquake in 2008 in China. In reality, interruptions in their operations often result in considerable social and economic damage at the regional or national level. For example, an initial disturbance in Ohio triggered the largest blackout in US history on 14 August 2003, causing an estimated $250–300 billion loss in total [2]. Due to the importance of CIs, it is very necessary to analyze complexity and vulnerability of them.

Complexity refers to the difficulty of identifying and quantifying causal links among a variety of specific adverse events and potential candidates [3]. CIs are often described as a complex set of interconnected, large scale, spatially distributed, interdependent, and adaptive systems upon which society, manufacturing systems, and residents depend. Moreover, CIs gradually become more and more complex and mutually dependent along with developments in science

and technology. Because CIs are composed of a great diversity of interacting subsystems and components, even small perturbations or interferences can trigger large scale and harmful consequences. The issue of extending modeling and simulation techniques is addressed by Kröger [4], for the purpose of coping with the increasing complexity. Once part of a CI is disturbed or even collapsed, the adverse effects may rapidly diffuse directly or indirectly to other components or even spread to other infrastructures. In some cases, serious accident may be derived just from a minor failure of some components [5]. For example, the 22 June 2009 Washington metro collision, which resulted in the death of 9 people, the injury of 52 people, and economic losses of about 12 million dollars, was triggered by an initial fault in signal system. Moreover, the dramatic events like terrorist attacks have particularly long-lasting and far-reaching effects on the society, such as those that happened in 2004 in Madrid, in 2005 in London, and in 2010 in Moscow [6]. Hence, it can be said that capturing complexity of CIs will provide an important foundation for CIs safety operation.

The operation safety of CIs is decisive for the strategy of country industrial development, economic growth, and public confidence. Many researches have been carried out in a variety of critical infrastructures from different perspectives, such as high-speed railway [7], power plant [8], road network [9], and water supply system [10]. The existing studies mainly focus on the safety evaluation and improvement, risk identification and prediction, interference factors analysis and controlling, and system optimization by using comprehensive approach and general method. With the increasing of complexity and hazards, there is a need to develop new perspective or approach for infrastructure safety. In the context of the existing literature, some attention is already paid to vulnerability of infrastructure system [11–13]. Vulnerability analysis is applied within the management of CIs and some achievements have been made by exploring the impacts of random disturbances, deliberate attacks, and natural disasters. For instance, indicators have been proposed to quantify the redundancy of water distribution systems by assessing their tolerance of random failures and targeted attacks [14]. Furthermore, vulnerability analysis is also quite beneficial for decision-making in case of an emergency [15]. Risk and vulnerability analyses are principal methods and essential tools for conducting proactive and effective safety management [16]. Therefore, it is increasingly needed to identify potential risk and vulnerability, which is the basis of establishing various related strategies and adopting a series of corresponding management and technical countermeasure [17]. However, the current study on vulnerability mainly targeted the infrastructure with a fixed topological structure, such as traffic network and power network. Little attention is paid to the infrastructure system itself without a fixed topological structure, and the systematic quantification of the internal structure vulnerability analysis to various hazards and failures is worthy of being pondered deeply.

The objective of this study is to explore complexity and analyze vulnerability in critical infrastructure system without a fixed topological structure, with the hope of offering new perspectives and ideas for managers to implement effective safety management. Engineering breakdown structure (EBS) and complex network theory (CNT) are employed to do the complexity and vulnerability analysis in this study. Metro system is considered as a typical case study due to its critical role in urban development and change. It is apparent that increasing complexities and interconnectivities are making metro system more in need of systematic vulnerability analysis. A specific data set is established by merging data obtained from various sources. The analysis is conducted by the proposed methodological approach. This study contributes to the existing literature on infrastructure safety in terms of potential research perspective and suitable modeling techniques.

The remainder of this paper is organized as follows. In Section 2, a literature review is presented on vulnerability of infrastructure and approaches to studying the vulnerability of infrastructure systems. Subsequently, the proposed modeling approach is explained and network analysis method is expatiated in Section 3. Next, a case study is executed in which the metro physical network's topological properties are discerned in accordance with degree, betweenness, average path length, network diameter, and clustering coefficient. The system's vulnerability to component failure is then determined through the failure analysis of network nodes and edges. Furthermore, in Section 5, final comments summarize conclusions and suggestions concerning possible implementation issues and future study.

2. Literature Review

2.1. Approaches to Study Infrastructure System. Numerous efforts have been carried out by academia and practitioners to develop approaches capable of analyzing risk and vulnerability. The main methods in current vulnerability studies can be divided into two kinds, that is, empirical approach and predictive approach [18]. The main purpose of the empirical approach is to identify formation mechanisms and patterns of cascading failure and its consequences, assisting in gaining knowledge or experience through the analysis of previous near-miss and accidents. The predictive approach mainly refers to modeling or simulating the major characteristics of infrastructure system through reasonable simplification, aiming to analyze the potential hazards or consequences. Several representative research methods are expatiated as follows.

Agent-based modeling (ABM) is a relatively new approach to simulating infrastructure systems composed of different types of autonomous agents. This method is usually used to study the behavior of an infrastructure network and its relevant economic entity [19]. An agent is built with the information of a specific location, function, and behavior, which can be used to represent different components in infrastructure system. The ABM method is always employed to research infrastructure system in terms of specific scenarios. An agent-based model has been constructed to support infrastructure interdependencies assessment process in order to identify and mitigate significant risks arising from interconnections [20, 21].

Object-oriented modeling (OOM) is another method for characterizing and analyzing the dynamic behaviors of

infrastructure system. It can include physical rules in the simulation and emulate behavior emerging as a result of individual actions at a global level. It could be deemed as a modification or evolution of agent-based modeling. Behavior rules of individual are defined, and individuals can communicate with each other. Therefore, the global behavior characteristics emerge as a result of numerous individuals. OOM supports event-driven and time-dependent simulations and allows the explicit integration of highly nonlinear, time-dependent effects and nontechnical factors [22]. In this view, OOM obviously demonstrates its attractiveness in detailed simulating of infrastructures. OOM has been used as a simulation framework to discern the most vulnerable part of CI systems in numerous operational scenarios [23].

The System Dynamics (SD) approach is applicable to research into interdependent infrastructure systems by using stocks, flows, and feedback loops [24]. SD depends on the structure of the model, time lags, and amplification that occur through feedback. An innovative modeling and analysis framework has been proposed to study an entire infrastructure system by using an existing individual model together with SD, functional models, and nonlinear optimization algorithms [25]. Min et al. [25] also propose an innovative economic-SD model to study an entire system of physical and economic infrastructures. Rehan et al. [26] propose using a SD model to study the planning and management of water utilities infrastructure. Based on SD, Genge et al. [27] design a methodology for assessing the impacts of cyber-attack by changing control variables, which is responsible for correct functioning of operational process in infrastructures.

Input–output model is another methodology for studying infrastructure proposed by Leontief in 1973, which is able to describe the ripple effect of disruptions to interdependent systems [28, 29]. This approach is usually used to build the correlation between economic sectors and quantify the relationships between infrastructure networks. In this model, the interdependences are captured at a macro level rather than in a micro perspective, and elements of each infrastructure have not been analyzed in detail. Yu et al. [30] use a vulnerability measure that integrates information elicited from expert judgment to develop an input–output model, for studying the satisfaction of fuzzy economic output goals under conditions of scarcity caused by climatic disruptions. The case study in this research indicates that transportation, trade, and service-oriented industries suffer losses in gross domestic product (GDP). Although input–output model is helpful to assess vulnerability, it seems to be difficult to extend for restoration activities [19].

CNT is another widely used method to simulate the characteristics of infrastructures in specific analysis. Indeed, CNT has received increasing attention in recent years and is applicable to analyze and evaluate various properties of real infrastructures, such as vulnerability and reliability [31, 32]. It has been widely used with infrastructures in form of visible networking, such as power grid networks [33, 34], transportation networks [35, 36], and pipeline networks [37, 38]. In addition, graph theory and multiattribute utility theory have also been employed to identify and prioritize candidate infrastructure scenarios vulnerable to terrorist attack [39].

In addition, some other methods are also employed to study infrastructure system, such as entropy theory [40]. Sometimes, according to the characteristics of the research object, hybrid approach is adopted to implement the corresponding work. However, there is not a silver bullet solution for all applications in infrastructure system research; all these models and methods have their own advantages and shortcomings and the most suitable approach depends on the specific problems and conditions for each situation.

2.2. Vulnerability of Infrastructure. The word vulnerability comes from Latin, which is mainly used to describe the characteristic that the system and its components could be easily affected and destructed. For example, Achilles heel is a typical example of vulnerability. Recent literature reviews reflect a growing attention in the research of infrastructure vulnerability, and contributions are produced in various disciplines and applied in many different fields [41]. In current research, because different disciplines have their own characteristics, the definitions of vulnerability are always different, especially between natural science and social science, and sometimes they seem ambiguous [42]. Generally speaking, there are two commonly accepted interpretations in research literature [19]. One is that vulnerability is regarded as a system property which means the severity of consequences under the occurrence of a specific hazardous event [43]. The other is that vulnerability applies to express a critical system component, a geographical location, or an aspect of a system [39]. According to these interpretations, there are different types of vulnerability analyses, ranging from global vulnerability analysis [44] and critical component analysis [42] to critical geographical locations analysis [45].

In modern society, infrastructure system and its components do not exist in isolation and the functional or physical relationships between them are dynamic and complex. Due to interdependences inside the infrastructure or among infrastructures, the failure in any part of system will affect other parts or even spread and cause disturbances to other infrastructures through functional or physical connectivity [46]. As such, hazard or failure may give rise to unanticipated cascading consequences. In 2008, a south China snowstorm caused considerable damage to many infrastructures such as transportation and electricity, and most lost part or all of their functions, resulting in an estimated direct economic loss of 1516.5 billion RMB. In addition, functional interdependences among different infrastructures can lead to more serious consequences. For instance, the snowstorm caused loss of transportation, which threatened the supply of coal required by the electric power infrastructure for its generators. Subsequently, the lack of adequate power resources substantially reduced and delayed the rescue effort.

Vulnerability analysis focuses on identifying Achilles' heels in system that may be activated by random incidents, uncertain hazards, or unnoticed threats. There are various disturbances in the operating process of infrastructure systems, which can be broadly divided into two types: concrete disturbances such as snowstorms and abstract disturbances such as random component failures [47]. Vulnerability analysis is therefore widely applied in the management of CI

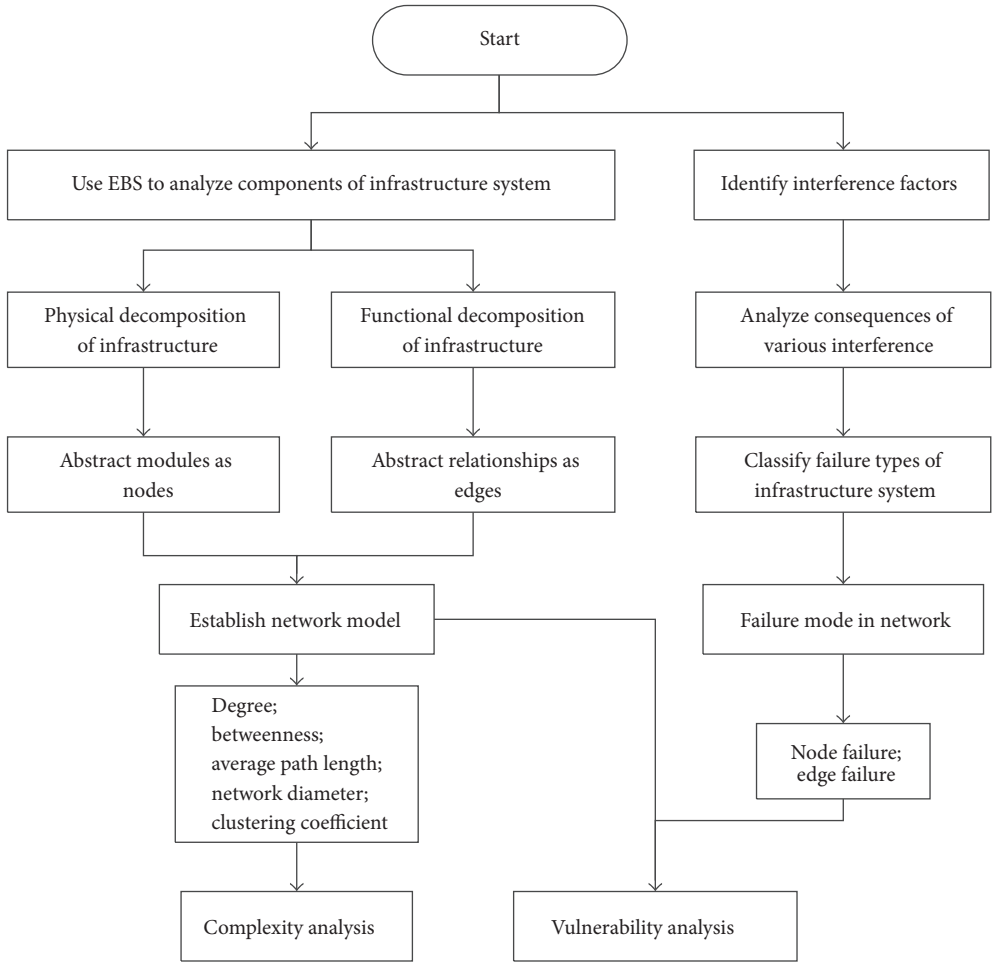


Figure 1: Framework for the complexity and vulnerability analysis.

systems in the form of evaluating the degree of adverse effects caused by the imposition of these disturbances.

3. Methodology

3.1. Proposed Framework. Along with the development of engineering technology, the physical structure and function of infrastructures have become increasingly advanced and complex. In general, an infrastructure usually consists of various physical subsystems and components. There are numerous interdependencies of differing kinds in infrastructures [48]. During their operation, these subsystems and components must work synergistically and collaboratively for producing and distributing a continuous flow of services or products. The relationships among components can be divided into two types, including physical relationship and functional relationship. From the perspective of network, if the components and their relationships could be discerned in an infrastructure, it could be established as network model. Therefore, CNT is the most appropriate method to analyze the complexity and vulnerability in this study.

According to the research purposes, a theoretic framework is proposed to study the complexity and vulnerability of infrastructure systems without a fixed topological structure. Based on the aforementioned idea, a particular framework is put forward and illustrated in Figure 1. As is known to all, node and edge are the two basic elements in a network model. Correspondingly, according to EBS, the node can be obtained by physical decomposition of infrastructure, and the edge can be obtained by functional decomposition. Based on the decomposition, the network model can be established to describe the infrastructure using network modeling technique. The topological properties in the network model can be analyzed to describe the complexity of the infrastructure. Then, failure types of infrastructure have to be identified for determining the failure mode, which is a key step to do vulnerability analysis in accordance with actual failure conditions.

According to the analytical framework, a prototype of collaborative network model can be built in generalized form by network analysis software *Pajek*, as illustrated in Figure 2. This network model can be used to vividly represent the components of CIs and their relationships.

3.2. Analytical Approach. With the continuous development of CNT, the statistical indexes of network structure have

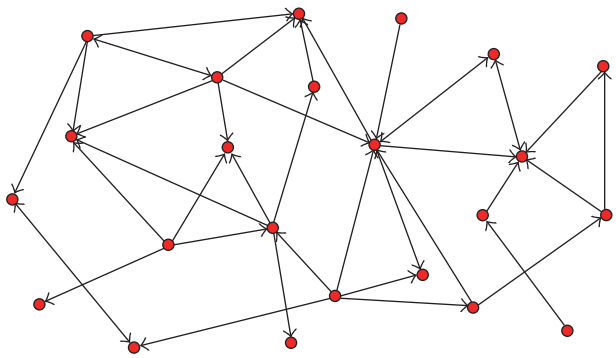


Figure 2: A prototype of collaborative network model.

obtained a lot of achievements, which are the basis of statistical description of various topological characteristics. Furthermore, calculation is usually precise and concise in research. In this paper, several typical indexes are employed to investigate the properties of infrastructure network, that is, degree, betweenness, average path length, network diameter, and clustering coefficient.

In general, for any network $G = (V, E)$, where $V = (v_1, v_2, \ldots, v_n)$ and $E = (e_1, e_2, \ldots, e_n)$, the degree of a node in a network is the number of edges connected to the node. In a directed graph, the degree can be either in-degree (number of incoming edges) or out-degree (number of outgoing edges), with the total degree being the sum of the two, which is expressed by (1). The degree distribution $P(k)$ is defined as the proportion of nodes with degree k, and the cumulative $P(k)$ is defined as the proportion of nodes equal to or greater than k [49]. Betweenness refers to the proportion of shortest paths through a node or an edge to the total shortest paths between all possible pairs of other nodes in a network. Two types of betweenness—"node betweenness" and "edge betweenness"—are used extensively in network analysis [50, 51]. Due to the similarity of node betweenness and edge betweenness, only node betweenness is used in this study, which can be calculated by (2) in which g_{st} denotes the length of the shortest path between node v_s and node v_t and $g_{st}(i)$ represents number of the shortest paths running through node v_i between node v_s and node v_t. The average path length is defined as the average number of steps between all possible pairs of nodes in a network, which could be described by (3). The network diameter is defined as the maximum path length in the network, which indicates the size of the network, which can be obtained by (4). The clustering coefficient is used to describe which nodes in a network tend to cluster together from a local perspective [52]. The clustering coefficient of a node is defined as the probability of two randomly selected neighbors of the node being connected, which can be calculated by (5), where e_i is the number of edges directly connected to node n_i.

$$k_i = \sum_{j \in N} e_{ij} \tag{1}$$

$$b_v(i) = \frac{1}{(N-1)(N-2)} \sum_{s^1 i^1 t} \frac{g_{s,t}(i)}{g_{s,t}} \tag{2}$$

$$L = \frac{1}{(1/2)N(N-1)} \sum_{i<j} \min_{i,j} d_{ij} \tag{3}$$

$$D = \max d_{ij} \tag{4}$$

$$C_i = \frac{2l_i}{k_i(k_i - 1)}. \tag{5}$$

Vulnerability is related to the capacity to continue operating following disruption; in other words, it can be described as the decrease degree of system efficiency after failure or attacks [53]. In a network, it could be interpreted as the degree of susceptibility to certain disturbances that may lead to reducing its functions. The critical element of a network (node or edge) is that most influence its vulnerability: the more critical the element, the greater the effects of its loss on the system [54, 55]. Each element of a network has its special functions although they are quite different. The vulnerability level of an element depends on the role it plays in the network structure. It is necessary to identify the weak points in the network for the sake of mitigating vulnerability [56]. In a particular case, such as catastrophic event, priority must be given to some critical nodes or edges over others to rebuild and recover the whole system [35].

Many definitions on system efficiency are created and studied, but they all have different limitation. At present, the generally accepted measure method is average reciprocal shortest path lengths of networks [57]. In network analysis, the vulnerability of a network G could be calculated by (6) [58], where d is the interference factor and D is the set of interferences. Φ denotes the functional metric and $\Phi[D(G, d)]$ denotes the degree of function loss. $\Phi(G)$ can be calculated by (7), where n is the number of nodes and d_{ij} is the distance between two nodes.

$$V(G, D) = \frac{\Phi[G] - \Phi[D(G, d)]}{\Phi[G]} \tag{6}$$

$$\Phi(G) = \frac{1}{n(n-1)} \sum_{\forall i,j, i \neq j} \frac{1}{d_{ij}}. \tag{7}$$

4. An Illustration Example

With the rapid increase of urbanization in China, an increasing number of people move from the countryside to the cities. One effect of this is serious traffic congestion and environment pollution, which is detrimental to the healthy development of cities [59]. In view of this, the metro, with large-capacity and energy-saving, is increasingly becoming an effective solution for reducing traffic congestion in large cities in China. As is known to all, China has many large and populous cities, with 142 cities being estimated to have populations over 1 million by 2015. The traffic pressure greatly stimulates the construction and operation of metro projects. At the end of 2015, metros in 24 Chinese mainland cities have already been put into operation with total mileage of 3010 kilometers, and many other cities have been authorized to build their urban metros. Nowadays, metro is becoming one

of the critical and essential infrastructures in China mainland, especially in the big cities such as Beijing, Shanghai, and Guangzhou.

The metro system is a good example for the case study in this paper. The metro physical network (MPN) model is established by a three-stage process. Firstly, the data of metro system is collected from monograph, literature, enterprise, and media. Many documents and webpages were downloaded and their contents are sorted and coded for content analysis. The achievement made in the first stage is to find out the components of metro system based on EBS method. In the second stage, an academic conference on the theme of relationships among components is held. Participating in the conference were leaders from the industry experts in metro equipment, some university professors, Nanjing metro operation company, and all the members of our research team. The physical or functional relationships among components are analyzed in-depth and coded in terms of the type and nature of the components. The potential methods of improving metro operation safety management are also discussed. In the third stage, *Pajek* is used to establish the MPN model in accordance with the components of metro system and their relationships. The nodes stand for components and the edges represent relationships. The entire MPN contains 30 physical modules, as shown in Table 1. Based on the aforementioned method, the MPN model is established, consisting of 30 nodes and 75 directional edges, as shown in Figure 3.

Table 1: Names and codes of physical modules.

Number	Physical module
(1)	Train system
(2)	High voltage network
(3)	Catenary system
(4)	Computer interlock
(5)	Dedicated communication
(6)	Optical fiber system
(7)	Clock system
(8)	Wireless communication
(9)	TV monitoring
(10)	Broadcast system
(11)	Automatic fare collection system
(12)	Screen doors
(13)	Escalator
(14)	Environment control system
(15)	Water supply and drainage system
(16)	Electrical and mechanical control system
(17)	Fire alarm system
(18)	Supervisory control and data acquisition
(19)	Passenger information system
(20)	Access control system
(21)	Screen display system
(22)	Sign system
(23)	Fire control system
(24)	Automatic train operation
(25)	Automatic train supervision
(26)	Automatic train protection
(27)	Track system
(28)	Building automation system
(29)	Low voltage network
(30)	Elevator

4.1. Analyzing the Complexity of MPN. Many studies show that the topology of a network plays a decisive role in the determining characteristics of a network [52, 60]. In a broad sense, calculating the topological parameter is helpful for acquiring complexity of the MPN and analyzing the spread of accidents [61]. Hence, five parameters of degree, betweenness, average path length, network diameter, and clustering coefficient are explored in this section, which can be used to describe the complexity of a network model from different perspectives.

4.1.1. Degree. The values of the in-degrees, out-degrees, and total degrees for the MPN are shown in Figure 4. The average degree value is 2.5, which indicates that each subsystem cooperates with two or three other subsystems on average in carrying out its function. The critical component failure will affect correlative components. Automatic train supervision (ATS) (vertex 25) has the highest degree of 13, with an 8 in-degree and 5 out-degree, which indicates that ATS plays a critical role in the whole metro system and is in a relatively central position. Its in-degree is also the highest in the network. Multiple paths make it difficult to control for operation safety, compared to other kinds of physical modules with low input degree. It is usually regarded as a key point in a network. The clock system (CS) (vertex 7) and building automation system (BAS) (vertex 28) have the next highest in-degrees with a value of 7. In daily operation, if a few high-degree nodes are attacked simultaneously, MPN will become vulnerable and be turned into a set of isolated subnetworks. Controlling these key nodes can have a positive influence on the robustness of the metro system, which is referential in equipment maintenance under the condition of limited security resource. In addition, it would be of great helpful to disrupt the connectivity among failures to prevent failures from spreading and propagating in MPN under special conditions.

Due to rare nodes with high degree, it makes little sense to analyze statistic data in the tail of the degree distribution. In practice, the cumulative $P(k)$ is preferred in statistical analysis using double logarithmic coordinate system, with the purpose of reducing statistical errors due to finite network size. The cumulative $P(k)$ of MPN is depicted in Figure 5 with approximate fit $P(k) = 2.1217 \times k^{-1.216}$, which basically follows the power-law. This indicates that the MPN has the property of scale-free according to CNT. The property means that MPN is robust to random attacks to some extent. The nodes with degree equal to or less than 4 account for 60%, and the influence of failure of these nodes on the network is relatively small. But MPN is vulnerable to simultaneous attacks aiming at nodes with high degree.

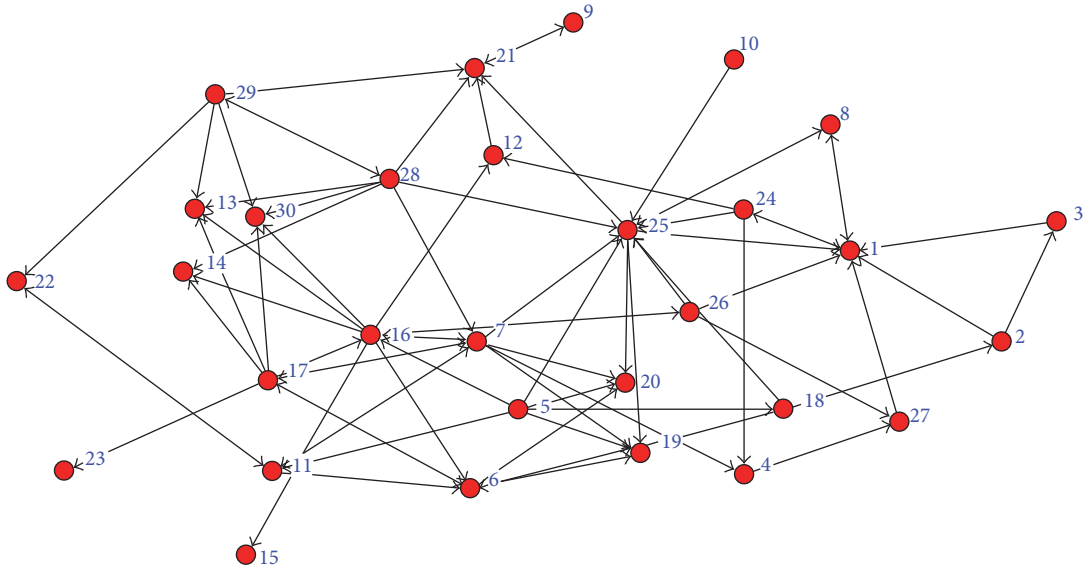


Figure 3: The network model of metro physical system.

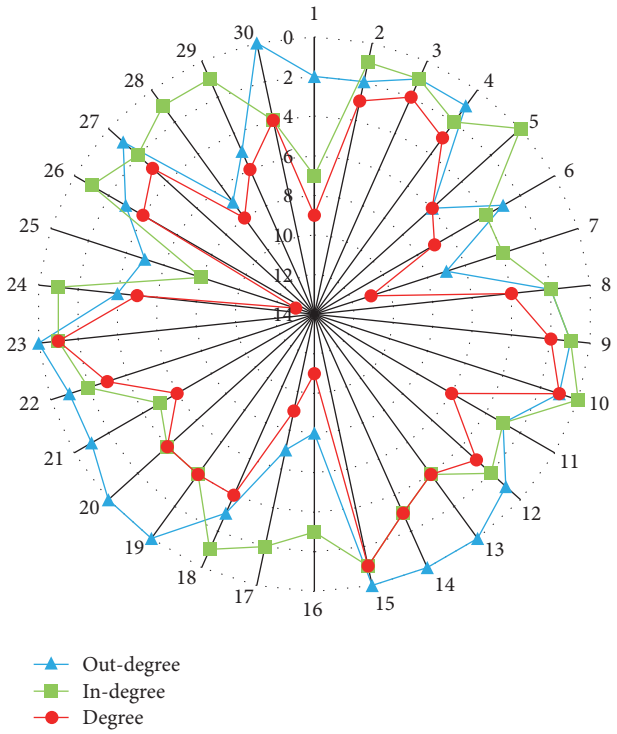


Figure 4: In-degree, out-degree, and total degree values.

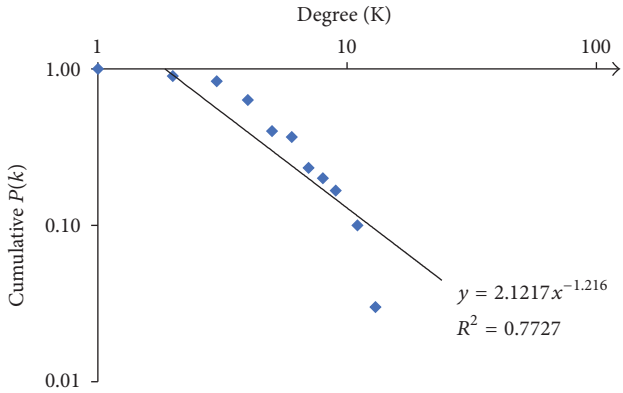


Figure 5: Cumulative degree distribution of MPN.

4.1.2. Betweenness. Node betweenness is used to describe the extent to which a node plays an intermediary role in the interaction between all possible pairs of nodes in a network [62]. Large node betweenness indicates greater importance in the whole network. The range of node betweenness in the MPN is 0 to 0.0976, as shown in radar chart in Figure 6. Eleven nodes are invisible due to their node betweenness being zero, which indicates that they do not play the role of intermediary among interactions between other nodes. The ATS (vertex 25) has the highest value of node betweenness, which means that the maximum number of shortest paths passes through ATS. Next CS (vertex 7) is 0.0963 and train system (TS) (vertex 1) is 0.0803. The cumulative node betweenness of these three nodes is equal to 0.2742, and almost about 40% shortest paths pass through these three nodes. These nodes should be paid more attention and maintenance cost in daily operation, and it is apparent that effectively controlling these few key nodes can slow down the failure diffusion and step down the chain reaction in MPN.

4.1.3. Average Path Length and Network Diameter. The transmission efficiency of information or energy has a significant correlation with the average path length, with shorter average path lengths having a higher efficiency. The value of the average path length in MPN is 2.5, which indicates that the information or energy is transmitted in two or three steps on average. For instance, TS (vertex 1) and computer interlock (CI) (vertex 4) are two isolated physical modules, which can be connected only in two steps, as presented in Figure 3.

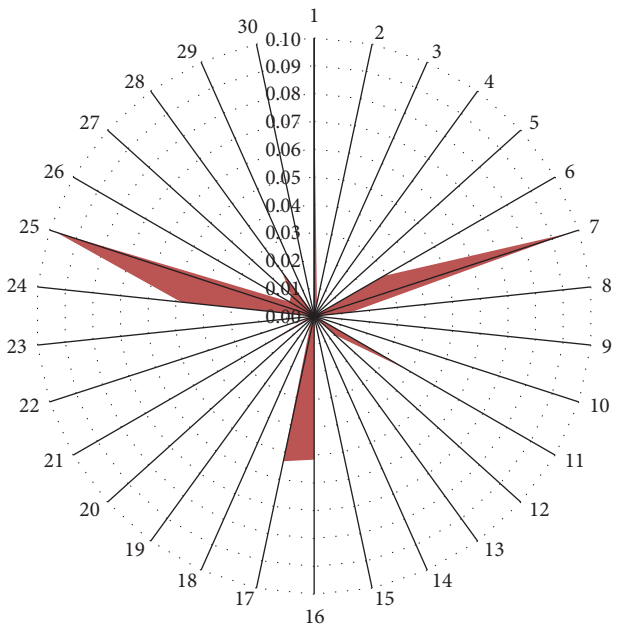


Figure 6: Betweenness of nodes in MPN.

In addition, the network diameter in the MPN is 6, which is from CI (vertex 4) to TV monitoring (TVM) (vertex 9). The MPN is therefore a relatively small network according to its average path length and network diameter. It means that metro system is a more collaborative network. In general, this kind of network always has a high operating efficiency, which means that MPN is an efficient transportation system.

4.1.4. Clustering Coefficient. The node clustering coefficient of the MPN is shown in Figure 7. It is observed that it only includes 22 nodes. The other eight nodes do not have a clustering coefficient because their in-degree or out-degree is equal to 1, which means they have only one adjacent node. In the process of calculating, the direction between nodes is not considered. The highest clustering coefficient is 0.5 (vertex 3 and vertex 8) and the lowest is 0.03 (vertex 6). The network clustering coefficient is defined as the average value of all nodes in the network and is 0.1085 in the MPN, which is larger than a random network with a similar network scale. The MPN has a short average path length and a high clustering coefficient, which indicates that it has small-world characteristics [63]. A small-world network is a special kind of graph in which most nodes can be reached from every other node by a short path. Failure propagation in MPN is much faster than a regular network. Hence, it is necessary and changeful to control cascading failure among physical modules for avoiding a serious consequence.

4.2. Analyzing the Vulnerability of MPN. There are various kinds of interference factors in the process of metro operation, such as severe weather, equipment failure, and unsafe behavior of passengers. However, no matter what kind of interference, the harmful results can be divided into two categories: module failure and relationship failure. Corresponding to the network model, the consequences

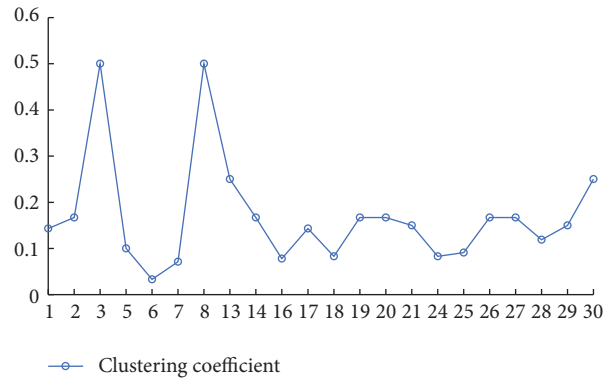


Figure 7: Values of clustering coefficient.

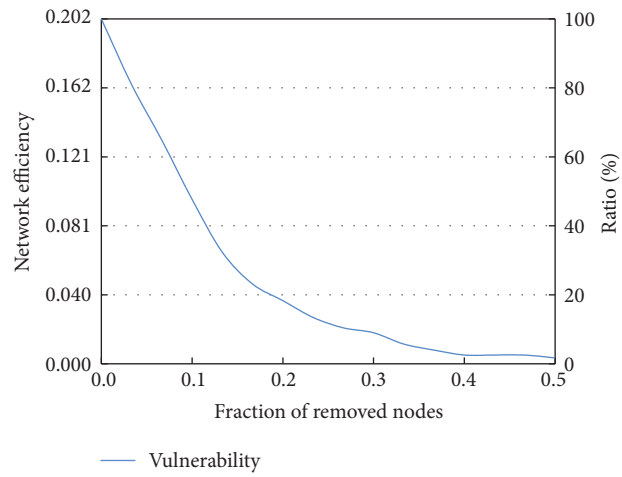


Figure 8: Changes of network efficiency with the largest degree node-based protocol.

are node failure and edge failure. Therefore, in this paper, vulnerability analysis is mainly implemented as follows.

4.2.1. Vulnerability in Node Failure Mode. Vulnerability in node failure mode is analyzed in this section. One node in the network model represents a physical module in critical infrastructure, and the whole network represents the whole infrastructure. If a module can not provide its normal function in reality, the corresponding node will be deleted from the network model. The deletion sequence of nodes corresponds with the order of node degree, called the "largest degree node-based protocol." Network efficiency is calculated in order to evaluate the change of performance in MPN. Figure 8 depicts the changes of network efficiency as the fraction of moved nodes increases, indicating that the network efficiency declines quickly as the number of removed nodes increases. The network efficiency is decreased by 60% when the fraction of removed nodes is about 10% and declines very quickly as it increases to 20%. This suggests that 10% of nodes with largest node degree are the most vulnerable nodes in the network model, which means that the corresponding components in the infrastructure are vulnerable. For instance, the most vulnerable module in the

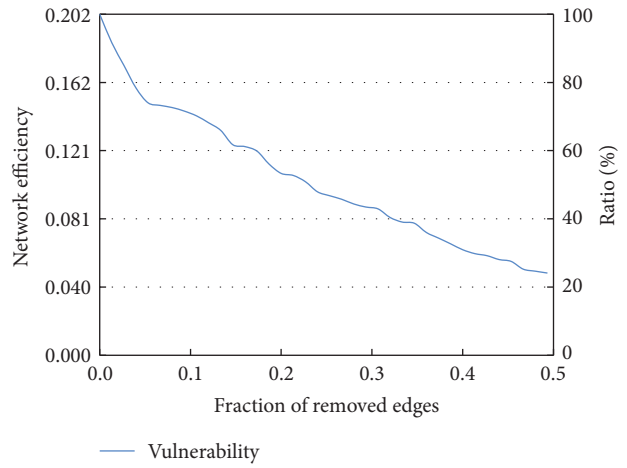


Figure 9: Changes of network efficiency with the highest betweenness edge-based protocol.

metro system is the ATS (vertex 25). If these critical modules can obtain good maintenance effect, the safety level in metro operation can be improved to a great extent.

4.2.2. Vulnerability in Edge Failure Sequences. Vulnerability in edge failure mode is analyzed in this section. One edge in the network model represents the functional relationship between two components in the infrastructure system. When an edge is unavailable to play its full part, the safest path between nodes will change due to forced detours around the failure. From this point of view, an edge will be deleted from the MPN model if the collaboration relationship is broken in reality. The deletion sequence of edges corresponds with order of edge betweenness, termed the "highest betweenness edge-based protocol." Figure 9 depicts the changes of network efficiency as the fraction of moved edges increases. Due to an edge just representing the partial function of one component, the curve declines slower under the edge deletion protocol comparing with the node deletion protocol. Network efficiency decreases by 20% when the fraction of removed edges is about 5% and declines at an even speed when this is larger than 10%. This indicates the most vulnerable relationship to be between the TS (vertex 1) and automatic train operation (ATO) (vertex 24) in MPN. If these critical relationships can obtain good maintenance effect, the safety level in metro operation can be improved to a great extent.

5. Conclusion and Discussion

In this paper, a theoretic framework is put forward to research critical infrastructure system without a fixed topology structure. Metro system is chosen to be investigated in accordance with network analysis, which is a powerful tool in complexity and vulnerability research. Based on the physical modules and their relationships, *Pajek* is selected to build the unweighted directed MPN. CNT is adopted to study the complexity and vulnerability of MPN. Five parameters including degree, betweenness, average path length, network diameter, and clustering coefficient are calculated and analyzed to better acquire and understand the network structure of MPN. These parameters reflect the topological properties from different perspectives, which is beneficial to understand and capture the complexity of metro system. ATS, CS, and TS are the three highest degree nodes in MPN, and about 40% shortest paths pass through these nodes. Effectively controlling these key nodes can reduce accident propagation efficiency and dampen chain reaction. The cumulative $P(k)$ of MPN obeys power-law distribution with the approximate fit $P(k) = 2.1217 \times k^{-1.216}$. It means that MPN has the property of scale-free network and is robust to random attacks. The properties of short average path length and big clustering coefficient denote that MPN has the property of small-world network. Accident propagation in this type of network is faster than random network and regular network. Meanwhile, it is found that metro system is a more collaborative network, and some few key nodes play a critical role in metro operation, such as ATS and TS. If some high-degree nodes are broken down or some high-betweenness edges fail to provide their normal function at the same instant, MPN is turned to be isolated and vulnerable. The key threshold is between 10% and 20%. The most vulnerable module in the metro system is the ATS, and the most vulnerable relationship is to be between the TS and ATO. These critical modules and relationships are Achilles' heels for the whole metro system. Effectively controlling these Achilles' heels can slow down the accident propagation and weaken chain reaction. Quantitative analysis of the topological parameters is beneficial to further understand and capture the complexity of MPN. The vulnerability analysis is helpful for controlling original accidents and avoiding secondary accidents. In view of the sequential relationships among numerous failures and accidents, this research may also have a positive impact on early-warning of accidents. In practice, the managers and technicians should pay more attention to the identified vulnerable modules and put more resource to assist in promoting safety performance in metro operation.

Because it is impossible to consider all failure factors due to their diversity and complexity, two removal strategies are selected to research the vulnerability of the metro system under the condition of real failures. According to actual situations, two different strategies are selected to evaluate performance change as measured by the network efficiency. The largest degree node-based protocol causes great damage to the metro physical network due to the nodes with large degrees having better local connectivity. In a real infrastructure system, this means these components exert a greater influence on a functional level. In contrast, the highest betweenness edge-based protocol causes relatively smaller but still serious damage. In a real infrastructure system, one edge represents the collaborative relationship between two components, which has less functional impact. Hence, through network analysis, the vulnerable components and functional relationships in MPN can be identified, and the extent of vulnerability can be obtained and quantified. It is envisaged that this study can help managerial personnel to understand the complexity and vulnerability in metro system for the sake of developing necessary strategies aimed

at improving safety management in a dynamic operating environment, especially in emergency.

The potential contributions of this study lie in three aspects. First, it helps to understand the complexity and vulnerability of infrastructure. In this paper, the main topology properties are captured in order to display the essential structure of metro system, and the vulnerability of metro system is analyzed. Second, network modeling technique is employed in this study, which may offer a possible approach to study complex infrastructure system. It will enlarge the application range of CNT. Furthermore, this study has the potential benefits in infrastructure emergency and relief. It can help managers to make decisions in emergency rescue in order to lighten the losses by original accident and avoid derivative or secondary accidents.

The main limitation of applying CNT in this study is that the established network model does not take the difference of nodes and edges into consideration. Various physical modules are collaborative to accomplish the overall functions of metro system, and it is very difficult to discern and distinguish the different importance for different physical modules; therefore, the weight is more difficult to assign. That is why the network model in this study is unweighted. In future study, more attention should be paid to improve the network model based on more precise understanding of infrastructure. Furthermore, how to reduce the vulnerability of infrastructure is a significant direction which deserved further research. In addition, the potential interdependencies among metro system and other CIs deserve more attention and should be explored systematically.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

The research described in this paper is supported by National Natural Science Foundation of China (51323004), the Humanities and Social Sciences Youth Foundation of China's Education Ministry (17YJCZH035), the Fundamental Research Funds for the Central Universities (2017QNB13), and Jiangsu Planned Projects for Postdoctoral Research Funds (1701143C).

References

[1] L. Masiero and R. Maggi, "Estimation of indirect cost and evaluation of protective measures for infrastructure vulnerability: a case study on the transalpine transport corridor," *Transport Policy*, vol. 20, pp. 13–21, 2012.

[2] J. Wang and L. Rong, "Cascade-based attack vulnerability on the US power grid," *Safety Science*, vol. 47, no. 10, pp. 1332–1336, 2009.

[3] O. Renn, A. Klinke, and M. Van Asselt, "Coping with complexity, uncertainty and ambiguity in risk governance: a synthesis," *Ambio*, vol. 40, no. 2, pp. 231–246, 2011.

[4] W. Kröger, "Critical infrastructures at risk: a need for a new conceptual approach and extended analytical tools," *Reliability Engineering and System Safety*, vol. 93, no. 12, pp. 1781–1787, 2008.

[5] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.

[6] E. Rodríguez-Núñez and J. C. García-Palomares, "Measuring the vulnerability of public transport networks," *Journal of Transport Geography*, vol. 35, pp. 50–63, 2014.

[7] W. Wei, M. Guo, L. Ye, G. Liao, and Z. Yang, "Work-family conflict and safety participation of high-speed railway drivers: job satisfaction as a mediator," *Accident Analysis and Prevention*, vol. 95, pp. 97–103, 2016.

[8] T. Aldemir, "A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants," *Annals of Nuclear Energy*, vol. 52, pp. 113–124, 2013.

[9] J. Wang and H. Huang, "Road network safety evaluation using Bayesian hierarchical joint model," *Accident Analysis and Prevention*, vol. 90, pp. 152–158, 2016.

[10] J. Seo, M. Koo, K. Kim, and J. Koo, "A Study on the probability of failure model based on the safety factor for risk assessment in a water supply network," *Procedia Engineering*, vol. 119, pp. 206–215, 2015.

[11] T. H. Grubesic and T. C. Matisziw, "A typological framework for categorizing infrastructure vulnerability," *GeoJournal*, vol. 78, no. 2, pp. 287–301, 2013.

[12] S. Marrone, R. Nardone, A. Tedesco et al., "Vulnerability modeling and analysis for critical infrastructure protection applications," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 3, pp. 217–227, 2013.

[13] S. Larocca, J. Johansson, H. Hassel, and S. Guikema, "Topological performance measures as surrogates for physical flow models for risk and vulnerability analysis for electric power systems," *Risk Analysis*, vol. 35, no. 4, pp. 608–623, 2015.

[14] A. Yazdani and P. Jeffrey, "A complex network approach to robustness and vulnerability of spatially organized water distribution networks," https://arxiv.org/abs/1008.1770.

[15] D. L. Banks, "Foundations of risk analysis: a knowledge and decision-oriented perspective," *Journal of the American Statistical Association*, 2012.

[16] S. Mu, H. Cheng, M. Chohr, and W. Peng, "Assessing risk management capability of contractors in subway projects in mainland China," *International Journal of Project Management*, vol. 32, no. 3, pp. 452–460, 2014.

[17] W. Kröger and E. Zio, *Vulnerable Systems*, Springer Science & Business Media, 2011.

[18] J. Johansson and H. Hassel, "An approach for modelling interdependent infrastructures in the context of vulnerability analysis," *Reliability Engineering and System Safety*, vol. 95, no. 12, pp. 1335–1344, 2010.

[19] S. Wang, L. Hong, and X. Chen, "Vulnerability analysis of interdependent infrastructure systems: a methodological framework," *Physica A: Statistical Mechanics and Its Applications*, vol. 391, no. 11, pp. 3323–3335, 2012.

[20] T. Brown, W. Beyeler, and D. Barton, "Assessing infrastructure interdependencies: the challenge of risk analysis for complex adaptive systems," *International Journal of Critical Infrastructures*, vol. 1, no. 1, pp. 108–117, 2004.

[21] A. Tolk and A. M. Uhrmacher, "Agents: agenthood, agent architectures, and agent taxonomies," *Agent-Directed Simulation and Systems Engineering*, pp. 75–109, 2009.

[22] M. Schläpfer, T. Kessler, and W. Kröger, "Reliability analysis of electric power systems using an object-oriented hybrid modeling approach," https://arxiv.org/abs/1201.0552.

[23] I. Eusgeld, W. Kröger, G. Sansavini, M. Schläpfer, and E. Zio, "The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures," *Reliability Engineering and System Safety*, vol. 94, no. 5, pp. 954–963, 2009.

[24] R. Rehan, A. J. A. Unger, M. A. Knight, and C. T. Haas, "Financially sustainable management strategies for urban wastewater collection infrastructure - Implementation of a system dynamics model," *Tunnelling and Underground Space Technology*, vol. 39, pp. 102–115, 2014.

[25] H.-S. J. Min, W. Beyeler, T. Brown, Y. J. Son, and A. T. Jones, "Toward modeling and simulation of critical national infrastructure interdependencies," *IIE Transactions (Institute of Industrial Engineers)*, vol. 39, no. 1, pp. 57–71, 2007.

[26] R. Rehan, M. A. Knight, C. T. Haas, and A. J. A. Unger, "Application of system dynamics for developing financially self-sustaining management policies for water and wastewater systems," *Water Research*, vol. 45, no. 16, pp. 4737–4750, 2011.

[27] B. Genge, I. Kiss, and P. Haller, "A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures," *International Journal of Critical Infrastructure Protection*, vol. 10, pp. 3–17, 2015.

[28] M. Leung, Y. Y. Haimes, and J. R. Santos, "Supply- and output-side extensions to the inoperability input-output model for interdependent infrastructures," *Journal of Infrastructure Systems*, vol. 13, no. 4, pp. 299–310, 2007.

[29] O. Jonkeren and G. Giannopoulos, "Analysing critical infrastructure failure with a resilience inoperability input-output model," *Economic Systems Research*, vol. 26, no. 1, pp. 39–59, 2014.

[30] K. D. S. Yu, K. B. Aviso, M. A. B. Promentilla, J. R. Santos, and R. R. Tan, "A weighted fuzzy linear programming model in economic input–output analysis: an application to risk management of energy system disruptions," *Environment Systems and Decisions*, vol. 36, no. 2, pp. 183–195, 2016.

[31] D. P. Chassin and C. Posse, "Evaluating North American electric grid reliability using the Barabási-Albert network model," *Physica A: Statistical Mechanics and Its Applications*, vol. 355, no. 2, pp. 667–677, 2005.

[32] J. Zhang, X.-B. Cao, W.-B. Du, and K.-Q. Cai, "Evolution of Chinese airport network," *Physica A: Statistical Mechanics and Its Applications*, vol. 389, no. 18, pp. 3922–3931, 2010.

[33] E. Bompard, E. Pons, and D. Wu, "Extended topological metrics for the analysis of power grid vulnerability," *IEEE Systems Journal*, vol. 6, no. 3, pp. 481–487, 2012.

[34] Y. Dai, G. Chen, Z. Dong, Y. Xue, D. J. Hill, and Y. Zhao, "An improved framework for power grid vulnerability analysis considering critical system features," *Physica A: Statistical Mechanics and Its Applications*, vol. 395, pp. 405–415, 2014.

[35] F. Bono and E. Gutiérrez, "A network-based analysis of the impact of structural damage on urban accessibility following a disaster: the case of the seismically damaged port au prince and carrefour urban road networks," *Journal of Transport Geography*, vol. 19, no. 6, pp. 1443–1455, 2011.

[36] K.-Q. Cai, J. Zhang, W.-B. Du, and X.-B. Cao, "Analysis of the Chinese air route network as a complex network," *Chinese Physics B*, vol. 21, no. 2, Article ID 028903, 2012.

[37] G. Lanzano, E. Salzano, F. S. De Magistris, and G. Fabbrocino, "Seismic vulnerability of natural gas pipelines," *Reliability Engineering and System Safety*, vol. 117, pp. 73–80, 2013.

[38] I. Bentes, L. Afonso, H. Varum et al., "A new tool to assess water pipe networks vulnerability and robustness," *Engineering Failure Analysis*, vol. 18, no. 7, pp. 1637–1644, 2011.

[39] G. E. Apostolakis and D. M. Lemon, "A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism," *Risk Analysis*, vol. 25, no. 2, pp. 361–376, 2005.

[40] P. Tamvakis and Y. Xenidis, "Comparative evaluation of resilience quantification methods for infrastructure systems," *Procedia-Social and Behavioral Sciences*, vol. 74, pp. 339–348, 2013.

[41] T. C. Matisziw, T. H. Grubesic, and J. Guo, "Robustness elasticity in complex networks," *PLoS ONE*, vol. 7, no. 7, Article ID e39788, 2012.

[42] H. Jönsson, H. Johansson, and J. Johansson, "Identifying critical components in technical infrastructure networks," *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, vol. 222, no. 2, pp. 235–243, 2008.

[43] M. Dilley and T. E. Boudreau, "Coming to terms with vulnerability: a critique of the food security definition," *Food Policy*, vol. 26, no. 3, pp. 229–247, 2001.

[44] J. Johansson, H. Jönsson, and H. Johansson, "Analysing the vulnerability of electric distribution systems: A step towards incorporating the societal consequences of disruptions," *International Journal of Emergency Management*, vol. 4, no. 1, pp. 4–17, 2007.

[45] S. A. Patterson and G. E. Apostolakis, "Identification of critical locations across multiple infrastructures for terrorist actions," *Reliability Engineering and System Safety*, vol. 92, no. 9, pp. 1183–1203, 2007.

[46] P. Trucco, E. Cagno, and M. De Ambroggi, "Dynamic functional modelling of vulnerability and interoperability of Critical Infrastructures," *Reliability Engineering and System Safety*, vol. 105, pp. 51–63, 2012.

[47] J. Johansson, H. Hassel, and E. Zio, "Reliability and vulnerability analyses of critical infrastructures: Comparing two approaches in the context of power systems," *Reliability Engineering and System Safety*, vol. 120, pp. 27–38, 2013.

[48] A. Vespignani, "Complex networks: The fragility of interdependency," *Nature*, vol. 464, no. 7291, pp. 984-985, 2010.

[49] S. Ghosh, A. Banerjee, N. Sharma et al., "Statistical analysis of the Indian Railway Network: a complex network approach," *Acta Physica Polonica B, Proceedings Supplement*, vol. 4, no. 2, pp. 123–138, 2011.

[50] A. Abbasi, L. Hossain, and L. Leydesdorff, "Betweenness centrality as a driver of preferential attachment in the evolution of research collaboration networks," *Journal of Informetrics*, vol. 6, no. 3, pp. 403–412, 2012.

[51] A. M. M. González, B. Dalsgaard, and J. M. Olesen, "Centrality measures and the importance of generalist species in pollination networks," *Ecological Complexity*, vol. 7, no. 1, pp. 36–43, 2010.

[52] E. Almaas, R. V. Kulkarni, and D. Stroud, "Characterizing the structure of small-world networks," *Physical Review Letters*, vol. 88, no. 9, Article ID 098101, 2002.

[53] M. Ouyang, L. Hong, Z.-J. Mao, M.-H. Yu, and F. Qi, "A methodological approach to analyze vulnerability of interdependent infrastructures," *Simulation Modelling Practice and Theory*, vol. 17, no. 5, pp. 817–828, 2009.

[54] M. A. P. Taylor, S. V. C. Sekhar, and G. M. D'Este, "Application of accessibility based methods for vulnerability analysis of strategic road networks," *Networks and Spatial Economics*, vol. 6, no. 3-4, pp. 267–291, 2006.

[55] E. Jenelius and L.-G. Mattsson, "Road network vulnerability analysis of area-covering disruptions: A grid-based approach with case study," *Transportation Research Part A: Policy and Practice*, vol. 46, no. 5, pp. 746–760, 2012.

[56] A. Chen, C. Yang, S. Kongsomsaksakul, and M. Lee, "Network-based acessibility measures for vulnerability analysis of degradable transportation networks," *Networks and Spatial Economics*, vol. 7, no. 3, pp. 241–256, 2007.

[57] R. Criado, A. García del Amo, B. Hernández-Bermejo, and M. Romance, "New results on computable efficiency and its stability for complex networks," *Journal of Computational and Applied Mathematics*, vol. 192, no. 1, pp. 59–74, 2006.

[58] P. Crucittia, V. Latorab, M. Marchioric, and A. Rapisarda, "Efficiency of scale-free networks: error and attack tolerance," *Physica A: Statistical Mechanics and Its Applications*, vol. 320, pp. 622–642, 2003.

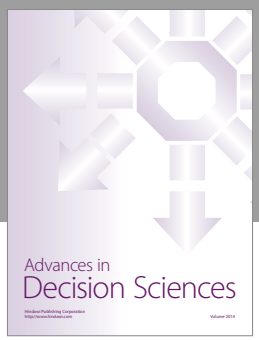
[59] J. Zhang, X. Xu, L. Hong, S. Wang, and Q. Fei, "Networked analysis of the Shanghai subway network, in China," *Physica A: Statistical Mechanics and Its Applications*, vol. 390, no. 23, pp. 4562–4570, 2011.

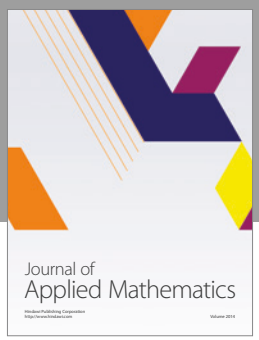
[60] A. Beygelzimer, G. Grinstein, R. Linsker, and I. Rish, "Improving network robustness by edge modification," *Physica A: Statistical Mechanics and Its Applications*, vol. 357, no. 3, pp. 593–612, 2005.

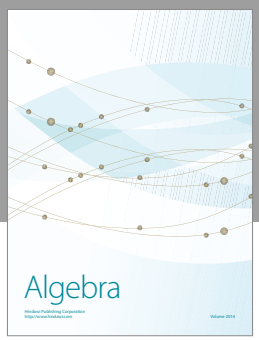
[61] Z. Zhou, J. Irizarry, and Q. Li, "Using network theory to explore the complexit of subway construction accident network (SCAN) for promoting safety management," *Safety Science*, vol. 64, pp. 127–136, 2014.

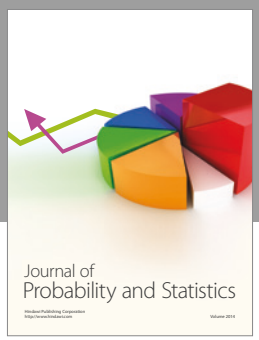
[62] B. W. Wambeke, M. Liu, and S. M. Hsiang, "Using Pajek and centrality analysis to identify a social network of construction trades," *Journal of Construction Engineering and Management*, vol. 138, no. 10, pp. 1192–1201, 2011.

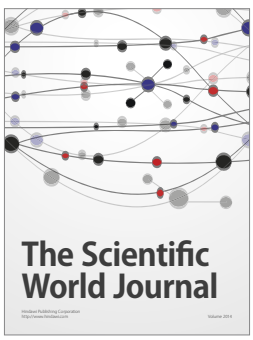
[63] D. J. Watts and S. H. Strogatz, "Collective dynamics of "small-world" networks," *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.

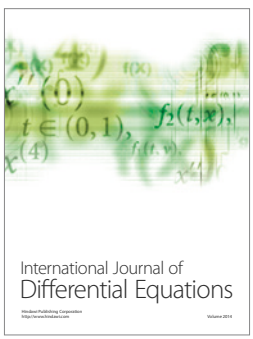


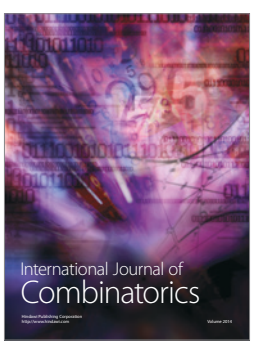


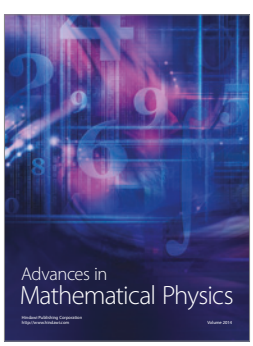


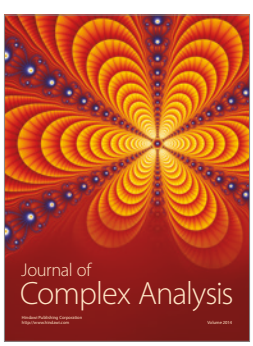


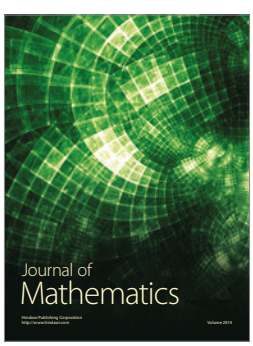


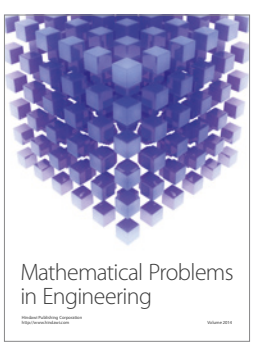


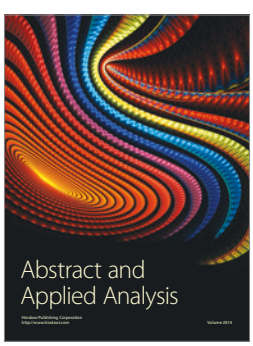


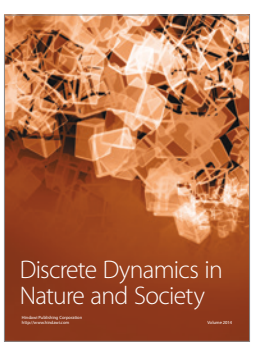


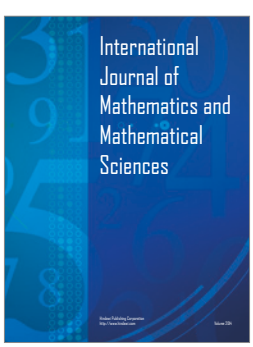


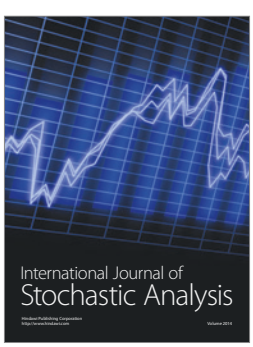












Hindawi

Submit your manuscripts at
https://www.hindawi.com