Hindawi
Advances in Civil Engineering
Volume 2021, Article ID 6658299, 12 pages
https://doi.org/10.1155/2021/6658299

Research Article

Invulnerability Simulation of Urban Agglomeration Passenger Transport Network under Incomplete Information Attack Strategy

Chengbing Li,[1,2] Zhicheng Yang,[3] and Yuan Zhu [1,2]

[1]*Transportation Institute, Inner Mongolia University, Hohhot 010021, China*
[2]*Inner Mongolia Engineering Research Center for Urban Transportation Data Science and Applications, Hohhot 010021, China*
[3]*School of Traffic and Transportation, Beijing Jiaotong University, Beijing 100044, China*

Correspondence should be addressed to Yuan Zhu; zhuyuan@imu.edu.cn

Received 12 October 2020; Revised 13 February 2021; Accepted 2 March 2021; Published 18 March 2021

Academic Editor: Hui Yao

This paper explores the invulnerability of urban agglomeration transportation network under the incomplete information attack strategy. This approach employed the site mapping method to construct the urban agglomeration composite transportation network model, and the network is weighted based on the actual passenger flow. Then the nodes are defined according to the overload conditions. In addition, based on the capacity-load model, the cascading failure model of the urban agglomeration passenger transport network is constructed, and the incomplete information attack strategy and network invulnerability measure index are determined. Finally, the case of Hu-Bao-E-Yu urban agglomeration is simulated to quantify the effects of attack strategies with varied information level, node load factors, and capacity weight and distance weight of the residual connected edge. The results reveal that the network crash speed is positively related to the information span of the attacker unless the information span exceeds 0.9 or accuracy exceeds 0.6. When the information span is low, the information accuracy δ has a critical impact on the network crash speed. Moreover, in the presence of attack, high or low values of node load factor are conducive to the improvement of network invulnerability. As a scale-free network, urban agglomeration transportation network shows strong robustness to random attacks and exhibits vulnerability to deliberate attacks. The capacity weight value α and distance weight value β of residual connected edge have different effects on the network invulnerability under different information span strategies.

1. Introduction

In the process of urbanization, urban agglomeration gradually replaced single city as the basic unit of global competition and division of labor [1]. The multimodal transportation network provides movement for the people and cargoes among cities in the urban agglomeration. Meanwhile, the increasingly complex transportation network is also facing the threats of passenger flow surge, natural disasters, terrorist attacks, etc. Once a component in the urban agglomeration is malfunctioning, the passengers and cargoes have to disperse into the surrounding components, affecting their operations, and then deteriorate the whole urban agglomeration transportation network. Therefore, it is crucial to improve the resilience of urban agglomeration transportation network under sudden disasters and deliberate attacks, particularly the cascading failure phenomenon of urban agglomeration transportation network.

Various research studies have been added to the literature works regarding the cascading failure of complex network. Luo and Zhang proposed a cascade failure model based on local priority redistribution rules with the consideration of the difficulty in implementing traditional shortest path routing under load distribution strategy in reality [2]. Ren et al. defined a random failure model in which the failure probability of each unit is related to the overload degree [3]. Plietzsch et al. defined a new cascading

failure model to observe the recovery power of electricity grid system under cascading failures by adjusting global and local redundancy [4]. Yin et al. analyzed the influence of node capacity by establishing a cascading failure model of scale-free network based on node degree [5]. Similarly, there are some research flows focusing on the capacity and load distribution [6–10].

On the other hand, the research to explore the impact of different attack strategies on the cascading failure process was widely carried out. Wang et al. analyzed the influence of two attack strategies on the robustness of cascading failures when the nodes are attacked in increasing or decreasing order in terms of the connectivity degree [11]. Based on the traditional capacity-load model, the cascading failure scenario of the weighted bus network was constructed by Zhang et al. and the simulation results under three attack strategies proved the effectiveness of the cascade failure model [12]. In view of the lack of research on multinode attack strategy under the condition of incomplete information, Chaoqi et al. proposed three attack strategies with information of different levels, and the impacts are simulated and analyzed. The results showed different advantages of strategies under three conditions [13]. According to the characteristics of equipment support network, Tian and Zhang introduce information precision parameters and intelligence span parameters to construct a general attack strategy model of equipment support network under incomplete information. Simulation results revealed that the existence of a threshold of information degree and the impact of the attack reach the maximum level when the threshold is attained [14].

In addition, some scholars jumped out of the system of the single isolated network and turned their attention to a complex system. Chen et al. studied cascading failure of coupled networks [15]. Cai et al. established an interdependence model between power system and dispatching data network to analyze the complex influence of cascading faults [16]. Hong et al. studied the performance of interdependent network under random attacks [17]. In the transportation field, Wu et al. studied the cascading failure of the weighted transportation network in urban transportation [18], which tried to establish the dynamic relationship between cascading failures and large scale of complex traffic flows. Yan et al. constructed a complicated network based on the original traffic flow to study its dynamic characteristics [19]. Additional research focused on the invulnerability change of urban transit networks causing by cascading failure [20–22], especially on rail transit networks [23].

The abovementioned research on cascading failure is mostly from the perspective of topological data on large network and the impact of network structures and load distribution strategies. However, the research on the transportation network cascading failure is mostly based on single mode in urban area, with little mention of the interaction of multimodal traffic in an urban agglomeration. Recently, with the acceleration of regional integration, the study of urban agglomerations is becoming an emerging field of urban research [24]. In addition, network attacks are mainly divided into two categories, namely, deliberate and random attacks. Since the attacker may neither understand all information nor know nothing on the network, it is difficult to quantify the threat merely based on single attack. Therefore, this paper constructs a cascading failure model of agglomeration transportation network under the incomplete information attack strategy (the strategy to select target nodes and attack when network information is only partially known) based on the impact of information span, node load factor, and load distribution mechanism.

The contents of this paper are structured as follows. Section 2 constructs a weighted transportation network model on the actual traffic flow using the existing research methodologies [24, 25]. Section 3 introduces incomplete information attack strategy, load factor, residual capacity weight of connected edge, and spatial distance weight index to establish the cascading failure model of an urban agglomeration and proposes the measurement indicator of invulnerability. Section 4 simulates and analyzes the model based on the investigation data of Hu-Bao-E-Yu urban agglomeration. The approach is summarized in Section 5.

2. The Weighted Transportation Network Model of Urban Agglomeration

In the previous research of agglomeration transportation network proposed by the author of this paper, road mapping methods are used to construct the topological graph of transportation network with multiple modes, which is based on the features of wide geographical range and large coverage area. In the approach, the stations of various transportation modes are regarded as the nodes and the interconnected edges. To study the characteristics of the composite transportation network in urban agglomeration, the adjacent stations are merged into one node and different transportation networks of various transportation modes are composed [24, 25]. Based on the previous research, transportation network model is constructed using the composite concept. Firstly, the subnetwork of single transportation mode is constructed, respectively. Then the adjacent stations of different transportation modes in urban agglomeration are merged into one node to implement the passenger flow between different transportation modes. The weight of the new node is the sum of the merged nodes, and the set of neighbor nodes came from all the adjacent nodes from the original subnetwork. Due to the wide geographical area of urban agglomeration, it should be noticed that the sites with close distance often exist within the same city. The distance between these sites can be obtained through GIS technology, and the sites within 20 minutes range by walking or transit are merged into a composite node.

Based on the analysis above, the following assumptions are made for the composite network considering the realistic characteristics of urban agglomeration transportation network:

> Hypothesis 1: the urban agglomeration transportation network is an undirected network, which means the traffic from one node to another also used the same link to return, and the traffic flow is approximately the same.

Hypothesis 2: the passenger flow between any two stations in the urban agglomeration transportation network remains unchanged for a certain period.

Hypothesis 3: the stations are merged when passenger's transfer time between connected stations is short, and the merged node is denoted as a composite node. In addition, V' represents the set of nodes to be merged, and V'' is the set of composite nodes.

Hypothesis 4: if there are multiple edges connecting two nodes, they are regarded as one edge named composite edge. E' represents the set of edges to be merged, and E'' is the set of composite edges.

The composite transportation network model of urban agglomeration is denoted by $G(V, E, W, H)$, where V means the set of network nodes, $V = \cup_{s=1}^{q} V_s \backslash V' \cup V'' = \{v_1, v_2, \ldots, v_i, \ldots, v_n\}$. V_s represents the node set of the sth subnetwork, V' denotes the set of nodes to be merged, V'' is the set of composite nodes, q is the number of subnets, and n is the number of nodes of the composite network in urban agglomeration. E represents the set of edges corresponding to V, $E = \cup_{s=1}^{q} E_s \backslash E' \cup E'' = (e_{ij})_{n\times n}$. E_s denotes the edge set of the sth subnet, E' represents the set of edges to be merged, and E'' is the set of composite edges. When $v_i R v_j$, it means node v_i is connected with v_j, and $e_{ij} = 1$. When $v_i \overline{R} v_j$, it means node v_i is not connected with v_j, and $e_{ij} = 0$. $W = (w_{ij})_{n\times n}$ denotes edge weight matrix of transportation network in urban agglomeration, where w_{ij} is the weight of edge ij. $H = \{h_1, h_2, \ldots, h_i, \ldots, h_n\}$ denotes node matrix of transportation network, where h_i is the weight of node i.

This paper uses the actual passenger flow data of urban agglomeration transportation network to measure the edge weight, that is, the maximum daily passenger volume between these edges. Based on the number of maximum daily passenger aggregation in station, the maximum daily passenger volume of the node is corrected and used as the node weight. For the composite edge, the weight is the sum of combined edges weight of each subnet. For the composite node, the weight is the sum of merged nodes weights of each subnet.

3. The Invulnerability Analyses of Urban Agglomeration Transportation Network under Cascading Failure

3.1. The Cascading Failure Analysis of Urban Agglomeration Transportation Network. In reality, when a node or an edge of the network malfunctions due to an attack or natural disaster, the original load of the network is allocated to its adjacent nodes or edges according to certain rules. The reallocation may result in malfunctions of other nodes or links, and such chain reactions are called cascading failures. In the urban agglomeration transportation network, the failures of composite nodes and edges connecting multiple subnets will cause not only load redistribution of its own subnet but also the load change of some other subnets combined with it and eventually lead to the cascading failure of the entire composite transportation network in urban agglomeration.

The cascading failure model of the urban agglomeration transportation network is built based on the improved capacity-load model. The procedure is as follows:

Step 1: in urban agglomeration transportation network, assume that the capacity of node i is C_i, so $C_i = h_i$. L_i represents the initial load of node i with $\tau \times C_i = L_i$, and τ is node load factor with $0 \le \tau \le 1$. Similarly, the capacity of edge ij is C_{ij}, and $C_{ij} = w_{ij}$. L_{ij} denotes the initial load of edge ij. $\mu \times C_{ij} = L_{ij}$, and μ is edge load factor with $0 \le \mu \le 1$.

Step 2: under the incomplete information, the target node i is attacked.

Step 3: after node i fails, the node and its connected edge are deleted, and its load is redistributed to the adjacent nodes. The load distribution model is constructed by considering the distance and residual capacity of connected edges based on the attractiveness between lines caused by different redundant capabilities of connected edges and the spatial distance between connected and failed nodes. α is defined as the redundant capability weight of connected edge, β is spatial distance weight. When $\alpha + \beta = 1$, the failed node i distributes the load to the connected node, as shown in the following equation:

$$L_j(t+1) = L_j(t) + \left(\alpha \frac{C_{ij} - L_{ij}}{\sum_{j\in\Pi}\left(C_{ij} - L_{ij}\right)} + \beta \frac{d_{ij}}{\sum_{j\in\Pi} d_{ij}} \right) L_i(t), \tag{1}$$

where $L_j(t)$ is the load of node j at time t., C_{ij} represents the capacity of edge ij, L_{ij} denotes the load of edge ij, d_{ij} is the distance of edge ij, and Π represents the node set adjacent to node i.

Step 4: update the network load and determine the overloaded node. According to the difference between nodes load and capacity, the nodes are divided into three states: normal, pause, and failure, as shown in the following equation:

$$\text{If} \begin{cases} L_i < C_i \longrightarrow \text{normal} \\ L_i \ge C_i, \text{rand} > p_i \longrightarrow \text{pause} \\ L_i \ge C_i, \text{rand} \le p_i \longrightarrow \text{failure} \end{cases}, \tag{2}$$

where rand is the random number between 0 and 1 and $p_i = (L_i - C_i/C_i)$ is the failure probability of node i.

Step 5: identification of cascading failure occurrence. If there is a pause or failure node in the network, the cascade fails and goes to Step 6. Otherwise, there is no cascading failure, goes to Step 7.

Step 6: the redistribution of the load. For the failed node, redistribute load according to equation (1), and delete the node and its connected edges. For the pause node, only the excessive load is evacuated. The load distribution formula for the pause node i is as follows:

$$L_j(t+1) = L_j(t) + \left(\alpha \frac{C_{ij} - L_{ij}}{\sum_{j\in\Pi}\left(C_{ij} - L_{ij}\right)} + \beta \frac{d_{ij}}{\sum_{j\in\Pi} d_{ij}} \right) \times \left(L_i(t) - C_i(t)\right). \tag{3}$$

Go to Step 4.

Step 7: the judgment of attack end. If all the nodes in the network fail, the network is paralyzed, then the simulation ends, and the output is the invulnerability measure index (that is, to modify the relative scale of the largest connected subgraph; this index will be used to describe the degree of damage of the current network relative to the original network, and the change of the network's survivability can be determined by observing the change of this index). Otherwise, if the network nodes are not completely failed, go to Step 2 for the next round of attack.

The algorithm of this approach is presented in Figure 1.

3.2. Incomplete Information Strategy. Most of the existing research on complex network invulnerability used the random or deliberate strategy to investigate the network invulnerability. However, in urban agglomeration transportation network, due to the significant network coverage and the operation distance, the situation may become extremely uncertain. It is impossible for terrorists to know nothing or everything about the nodes and edges information of the transportation network. So, the selection of attack targets considers neither random attacks nor deliberate attacks. To describe the attacks on nodes in real network, this paper uses the incomplete information attack strategy to conduct the network attack.

The information index (λ, δ) is used to describe the degree of information acquisition of the network. The information span parameter $\lambda \in [0, 1]$ represents the level of understanding of the entire network. Assuming that there are N nodes in the network, if λN nodes with known information, deliberate attack strategy will be taken to attack these nodes, and $(1 - \lambda)N$ nodes with unknown information will be attacked by random attack strategy. It can be seen that when the parameter λ is higher, we know more about the network. The information accuracy parameter $\delta \in [0, 1)$ represents the acquisition of important node information. All nodes in urban agglomeration transportation network G are sorted in the descending order according to their weight, the sequence group $R = \{r_1, r_2, \ldots, r_i, \ldots, r_n\}$ is obtained, and the number of node v_i is r_i. ∇_i is defined as the information acquisition status of node v_i; when $\nabla_i = 1$, the weight of node v_i is certain; when $\nabla_i = 0$, the weight is unknown. Considering that the understanding of node information is often incomplete, so $\nabla \in [0, 1]$.

Here, the auxiliary variable π_i of the node v_i is introduced as follows:

$$\pi_i = r_i^{-(\delta/1-\delta)}. \tag{4}$$

Thus, the determination of known information nodes can be regarded as an unequal probability sampling problem. The probability of node v_i is ∇_i, as shown in the following equation:

$$\nabla_i = \frac{\pi_i}{\sum_{i=1}^{N}\pi_i} = \frac{r_i^{-(\delta/1-\delta)}}{\sum_{i=1}^{N} r_i^{-(\delta/1-\delta)}}. \tag{5}$$

Obviously, under the larger δ value, the node with larger weight will be selected easier. When $\nabla_i = (1/N)$, we randomly obtain the node information. When δ tends to 1, if $r_i = 1$, then $\nabla_i = 1$; if $r_i \neq 1$, then $\nabla_i = 0$, and the node with the highest weight is selected preferentially.

In conclusion, the method of unequal probability sampling is used to sequentially determine the set of known information nodes. Then, the set of known information nodes is attacked by deliberate strategy, and unknown information nodes are attacked by random strategy until the network is paralyzed.

3.3. Invulnerability Measure Indicator. Aiming at the features of wide area and large differences of passenger flow among nodes in urban agglomeration, this paper improves the traditional invulnerability measure indicator (the ratio of the number of effective nodes in the maximum connected subgraph before and after the attack), and the ratio of the sum of effective nodes load in the maximum connected subgraph before and after network attack is used as the new invulnerability measure indicator called the relative scale of the maximum connected subgraph, as shown in the following equation:

$$S = \frac{\sum_{i=1}^{N'} L_i}{\sum_{i=1}^{N} L_i}, \tag{6}$$

where N' represents the number of nodes in the maximum connected subgraph after the network is attacked, N denotes the number of network nodes without attack, and L_i represents the load of node i in the maximum connected subgraph. When the network is not attacked, the relative scale of the maximum connected subgraph is 1, and the network is in a fully connected state.

4. The Case Study

4.1. The Transportation Network Model Construction of Hu-Bao-E-Yu Urban Agglomeration. To demonstrate the impact of our model to an urban agglomeration network, the Hu-Bao-E-Yu urban agglomeration is taken as an example to simulate and analyze the abovementioned invulnerability model. Hu-Bao-E-Yu urban agglomeration is located in the inland area of northwestern China. The operation of large-scale passenger and cargo flow is mainly carried out through the railway and road transportation networks. Because of the limitation of the natural environment, there is no water transportation in Hu-Bao-E-Yu urban agglomeration. There are only three airports, which bear a small proportion of passengers and freight. Therefore, this paper takes all the bus

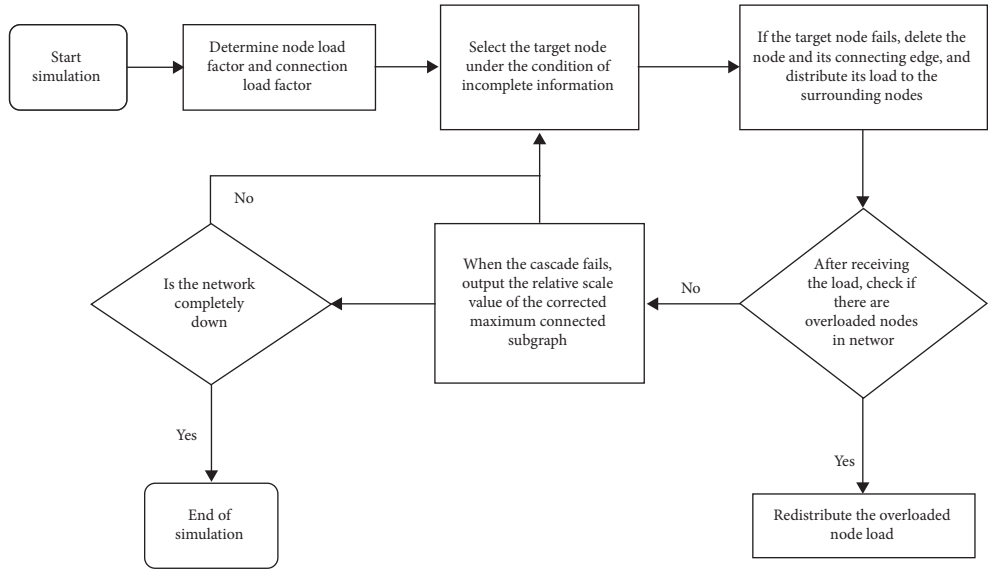

Figure 1: Algorithm flowchart.

stations and railway stations of Hu-Bao-E-Yu urban agglomeration as the nodes and the traffic lines as connected edges to construct the road transportation subnet G_1 and rail transportation subnet G_2. In this case, the road transportation subnet nodes $|V_1| = 263$, connected edges $|E_1| = 761$, and rail transportation nodes $|V_2| = 40$, connected edges $|E_2| = 164$. Furthermore, as mentioned above, the nodes where the passenger can transfer within 20 minutes are merged into a composite node [25]. And the composite transportation network model of urban agglomeration is constructed by combining road and rail transportation subnetworks. For the composite network, if there are multiple edges between two nodes, they are merged to be a composite edge. Here, nodes to be merged $|V'| = 36$, composite nodes $|V''| = 17$, and the composite transportation network nodes $V = V_1 \cup V_2 \cup V'' \backslash V'$, $|V| = 284$. The edges to be merged $|E'| = 104$, composite edges $|E''| = 57$, and the composite transportation connected edges $E = E_1 \cup E_2 \cup E'' \backslash E'$, $|E| = 878$. The composite nodes are shown in Table 1, and the transportation network topological graph of Hu-Bao-E-Yu urban agglomeration is shown in Figure 2.

Based on the transportation network model of Hu-Bao-E-Yu urban agglomeration, the distance between the stations is obtained through GIS, and the actual transportation data are obtained through the Inner Mongolia Transportation Administration, the Shaanxi Provincial Communications Department of Transportation Administration, and train stations. The initial node weight and connected edge weight are derived through the maximum daily passenger volume of nodes and edges. Further, the node weight is corrected by the value of the maximum daily passenger gathered on the station, and the capacity of each node is equal to the maximum daily passenger gathered on the station.

4.2. The Network Invulnerability Simulation under Incomplete Information Attack. In this paper, the impact of different attack strategies on the invulnerability of urban agglomeration transportation network is studied and simulated with MATLAB, which means that the values of information span parameter λ or information accuracy δ are changed on the basis of fixed parameters $\tau = 0.6$, $\mu = 0.6$, the connected edge residual capacity weight $\alpha = 0.5$, and the spatial distance weight $\beta = 0.5$. To substantiate the analysis, 50 nodes in the network are attacked, and the changes in the relative scale of the corrected maximum connected subgraph are captured. The simulation results are shown in Figure 3.

As shown in Figure 3, when the number of attacks increases, the relative scale of the corrected maximum connected subgraph decreases. It can be seen from Figures 3(a) and 3(b) that when the information accuracy is unchanged, the network crash speed (the degree to which the network's survivability measurement index drops for each attack on a node) increases with the information span. In particular, when the value of the information span λ reaches 0.9, continuous attack on 50 nodes can cause the global crash, and the relative scale of the corrected maximum connected subgraph becomes 0. When the information accuracy changes from $\delta = 0$ to $\delta = 0.2$, the acceleration speed of network collapse under different information span is different. According to Figures 3(a)–3(f), it is found that when the information span λ reaches 0.9, the network completely collapses after attacking 50 nodes, and the variation of the relative scale of the corrected maximum connected subgraph does almost not change with the change of the information accuracy value δ. This indicates that the attack strategy of the network has been optimal at this time. That is, the attack sequence of the node is almost certain, and at this point, the attack is almost a deliberate attack, under which the impact

Table 1: Composite nodes.

Normal node	Transportation network type	Composite node	Passenger's transfer time (min)
Hohhot coach station Passenger western station Hohhot railway station	Road transportation network Railway transportation network	Hohhot coach station-passenger western station-railway station	5
Yulin car passenger station Passenger south station Yulin railway station	Road transportation network Railway transportation network	Yulin car passenger station-passenger south station-railway station	10
Ordos bus station Ordos railway station	Road transportation network Railway transportation network	Ordos bus station-railway station	8
Dalad Banner bus station Dalad Banner railway station	Road transportation network Railway transportation network	Dalad Banner bus station-railway station	6
Chasuqi bus station Chasuqi railway station	Road transportation network Railway transportation network	Chasuqi bus station-railway station	3
Baotou coach station Baotou east railway station	Road transportation network Railway transportation network	Baotou coach station-east railway station	8
Suide bus station Suide railway station	Road transportation network Railway transportation network	Suide bus station-railway station	15
Dongsheng bus station Dongsheng railway station	Road transportation network Railway transportation network	Dongsheng bus station-railway station	11
Shenmu bus station Shenmu railway station	Road transportation network Railway transportation network	Shenmu bus station-railway station	13
Qingjian bus station Qingjian railway station	Road transportation network Railway transportation network	Qingjian bus station-railway station	3
Jinjie bus station Jinjie railway station	Road transportation network Railway transportation network	Jinjie bus station-railway station	10
Mizhi bus station Mizhi railway station	Road transportation network Railway transportation network	Mizhi bus station-railway station	5
Wubao bus station Wubao railway station	Road transportation network Railway transportation network	Wubao bus station-railway station	14

Table 1: Continued.

Normal node	Transportation network type	Composite node	Passenger's transfer time (min)
Dingbian bus station	Road transportation network	Dingbian bus station-railway station	15
Dingbian railway station	Railway transportation network		
Jingbian bus station	Road transportation network	Jingbian bus station-railway station	13
Jingbian railway station	Railway transportation network		
Zizhou bus station	Road transportation network	Zizhou bus station-railway station	14
Zizhou railway station	Railway transportation network		
Fugu bus station	Road transportation network	Fugu bus station-railway station	8
Fugu railway station	Railway transportation network		

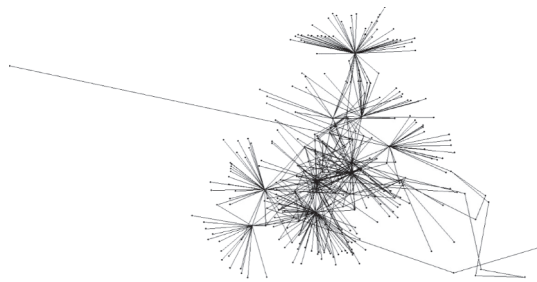

Figure 2: The topological graph of the road-railway composite transportation network of Hu-Bao-E-Yu urban agglomeration.

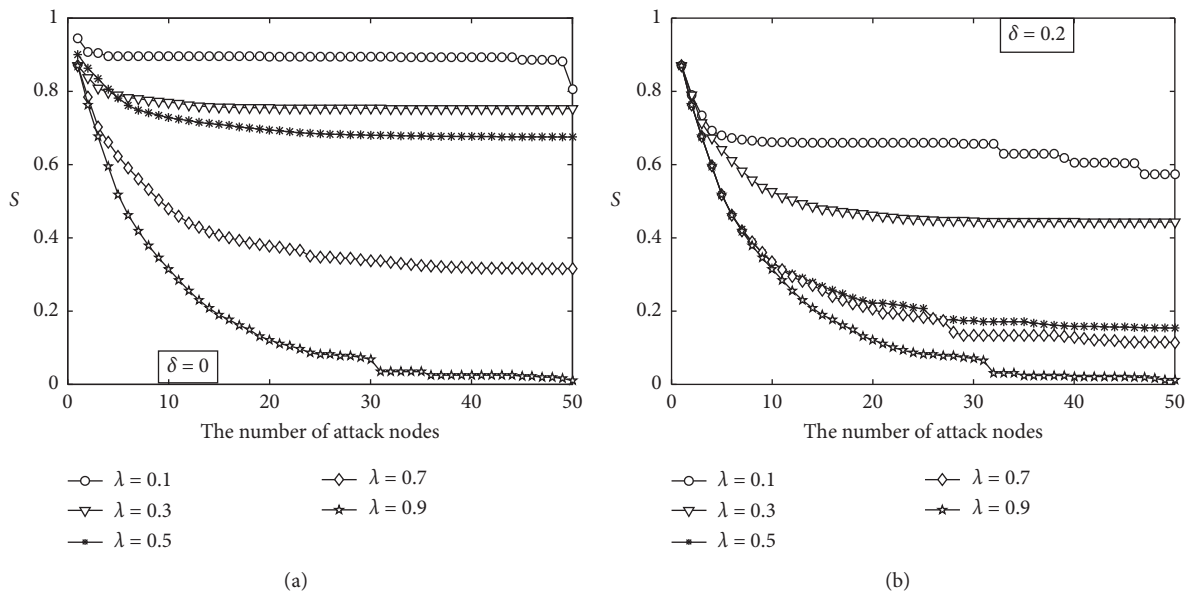

Figure 3: Continued.

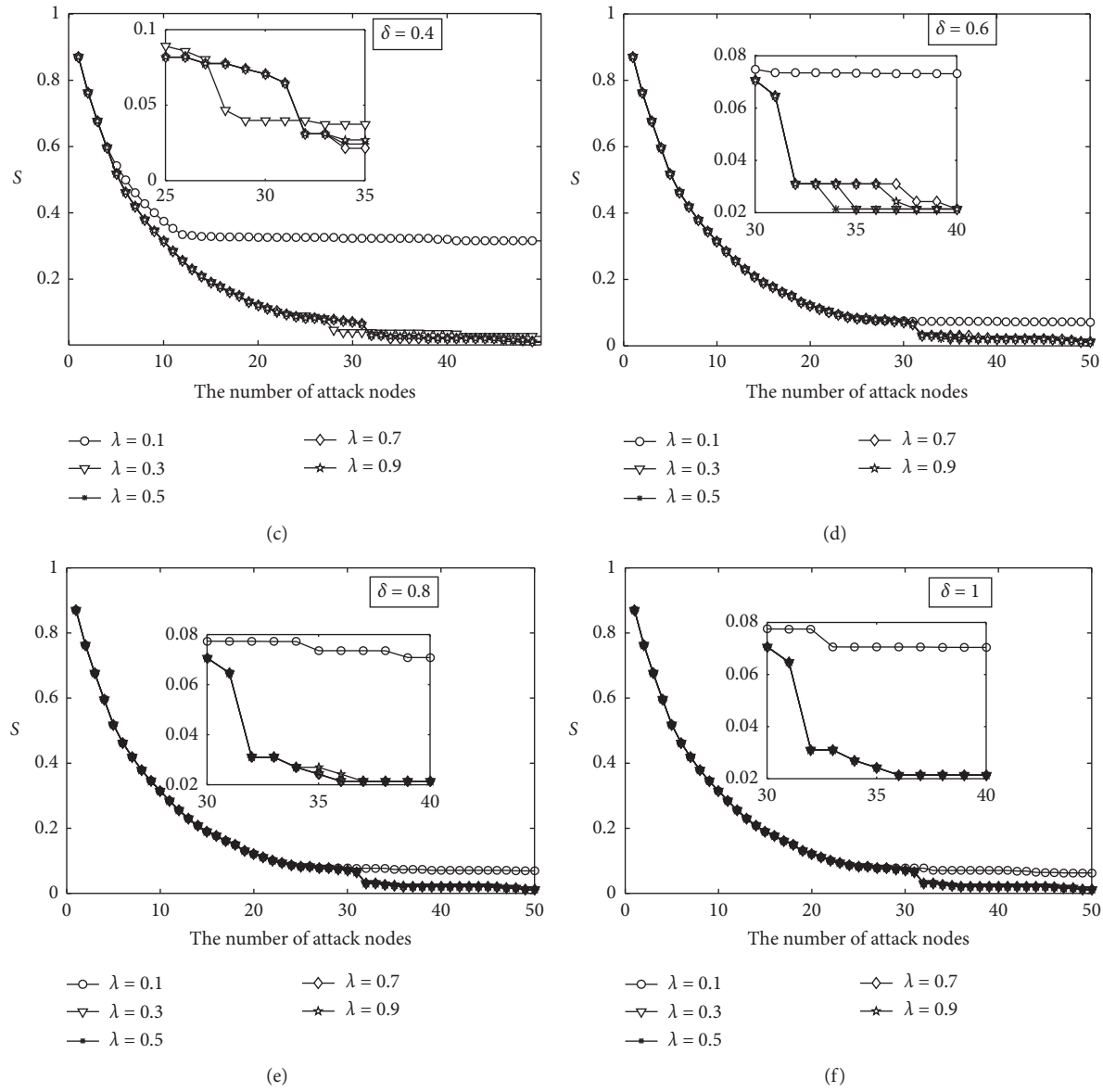

Figure 3: The simulation result of network invulnerability under different information conditions.

of the cascade failure is maximized. This shows that the impact of cascading failure will reach the maximum if the attack information span is 0.9. Therefore, the attacker does not need to obtain all the network information, but only needs to obtain the information that exceeded 0.9 to maximize the effect of the network attack. In addition, observing from Figures 3(d)–3(f), when $\lambda = 0.1$ and $\delta = 0.6$, no matter how the value of information accuracy δ changes, and the relative scale of the corrected maximum connected subgraph changes very little after the number of attack nodes reaching 30. This indicates that when the attacker obtains a small range of information, there is a threshold of the information accuracy. When the value is below the threshold, the network invulnerability does not change significantly.

4.3. Influence Analysis of Node Load Factor on the Network Invulnerability under Incomplete Information Attack. Under incomplete information attack, the influence of node load factor on network invulnerability is studied with the connected edge load factor $\mu = 0.6$, the residual capacity weight $\alpha = 0.5$, and spatial distance weight $\beta = 0.5$. Meanwhile, considering that information accuracy and information span are similar to each other in terms of their effects on invulnerability change, the information accuracy parameter is set to $\delta = 0.2$. The network invulnerability in different information span is observed by uniformly increasing the node load factor. The relative scale of the corrected maximum connected subgraph changes with the number of attack nodes, as shown in Figure 4.

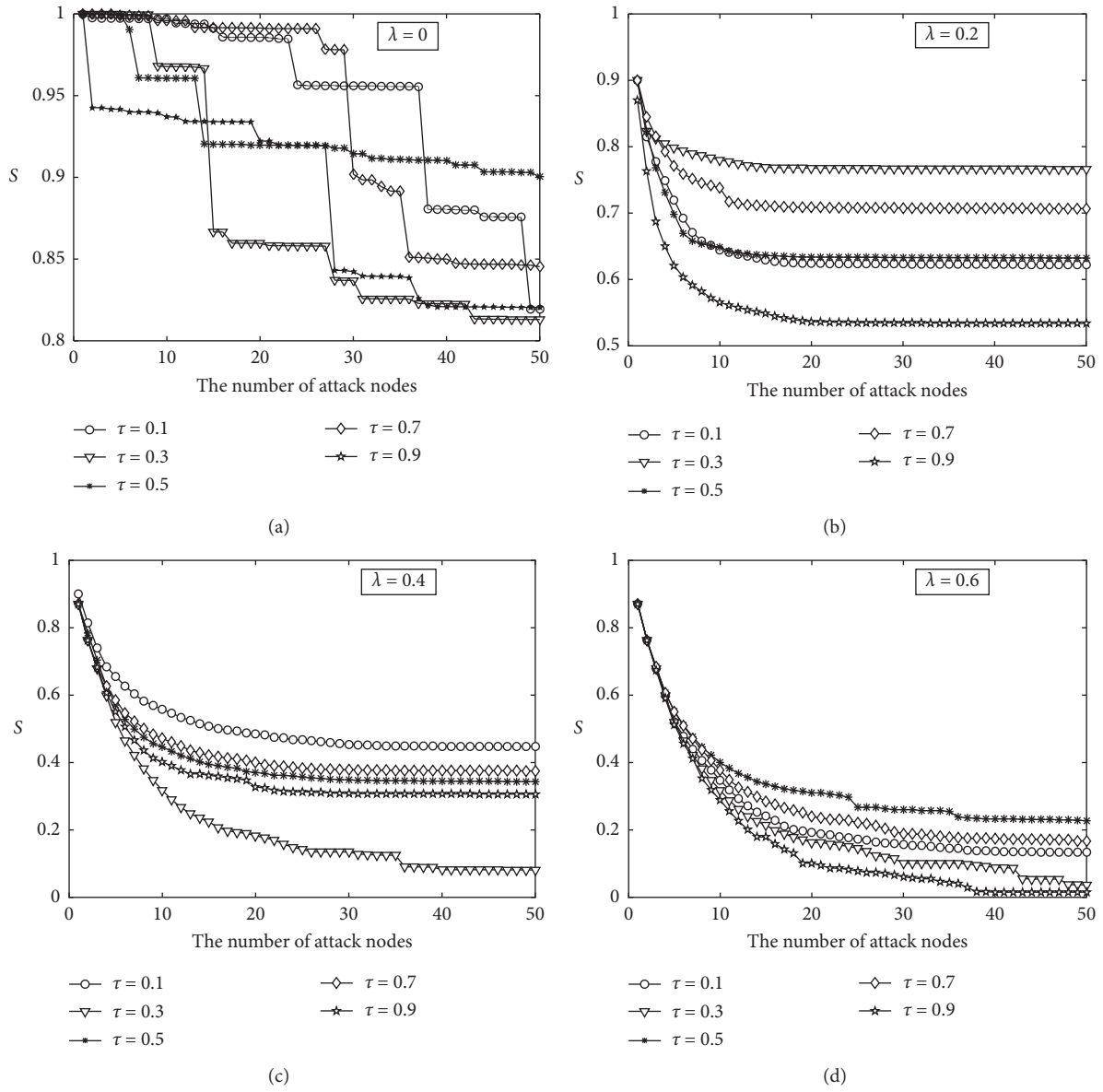

Figure 4: The simulation result of node load factor on urban agglomeration transportation invulnerability under different information conditions.

It can be seen from Figure 4(a) that when the information span parameter $\lambda = 0$, the attacker's access to network information is 0, which means that the attack sequence of the node is extremely irregular, and at this point, the attack is almost a random attack. Because the urban agglomeration transportation network has a wide geographical range and large coverage area and distinct capacity among stations, the relative scale of the corrected maximum connected subgraph is different. The network invulnerability is significantly influenced by a small number of important nodes. Once these stations are destroyed, the overall connectivity of the transportation network in urban agglomeration will be greatly affected. In addition, by comparing the scenarios, the urban agglomeration transportation network as a scale-free network shows strong robustness to random attacks but exhibits vulnerability to deliberate attacks. Comparing Figures 4(b)–4(d), we find that, under different information access degrees, the change of the relative scale of the corrected maximum connected subgraph shows different characteristics for distinct node load factors. Here, when $\lambda = 0.2$, the load factor $\tau = 0.3$ shows the strongest invulnerability. However, when the value of λ increases to 0.4 and the load factor $\tau = 0.3$, the network becomes highly vulnerable. No matter what the information span is, the network shows poor invulnerability to the load factor when $\tau = 0.9$. This indicates that the impact of the load factor on the network invulnerability is greatly affected by the attacker's access degree of information. If the redundant capacity of the station in the network is higher with a lower load factor, the invulnerability is not necessarily better.

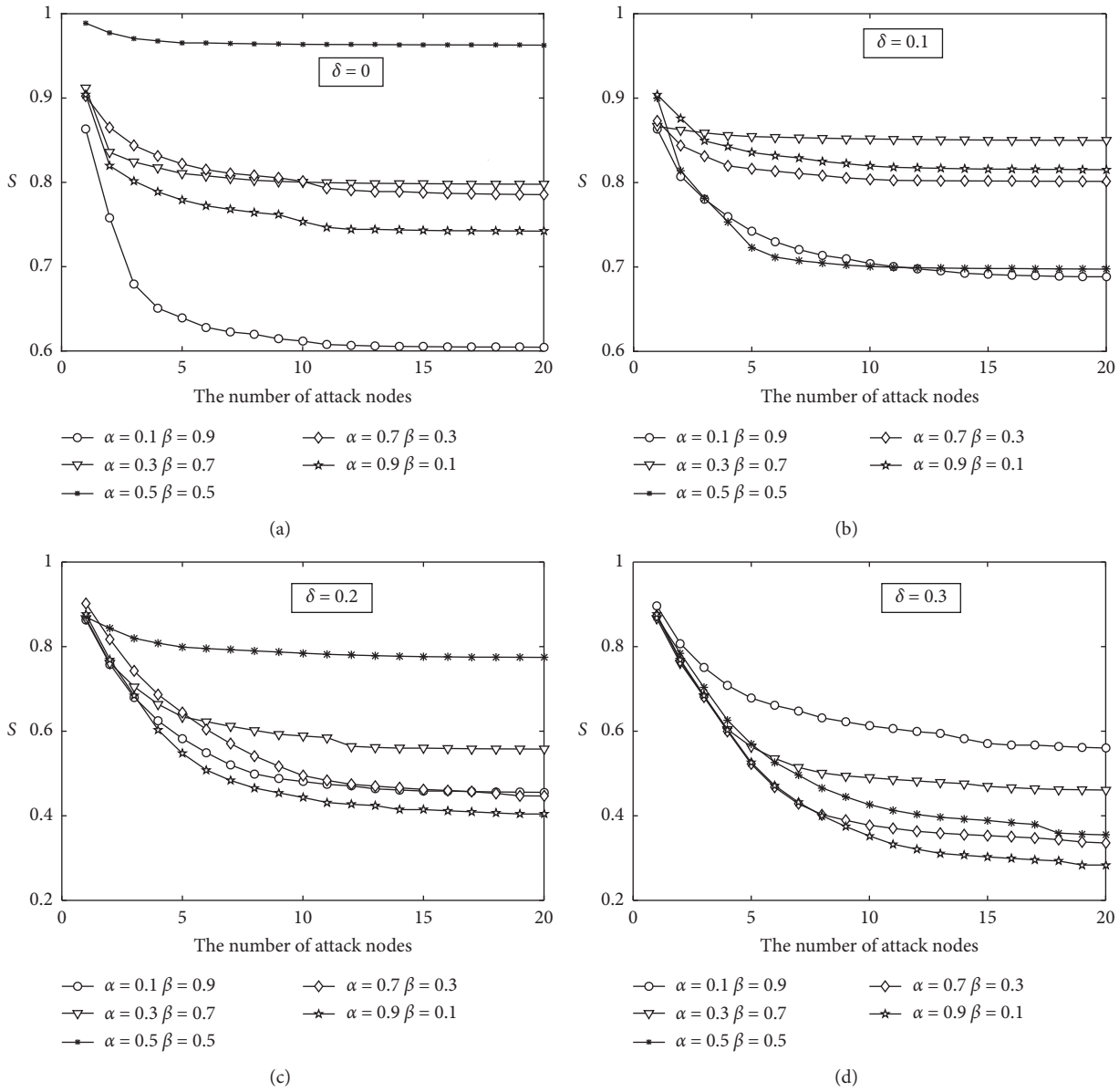

Figure 5: The simulation result of load distribution strategy on urban agglomeration transportation invulnerability under different information conditions.

4.4. Influence Analysis of Load Distribution Strategy on Network Invulnerability. By adjusting the values of residual capacity and spatial distance weights, this paper studies the effects of different load distribution strategies on network invulnerability during cascading failure. The node and connected edge load factor are set to $\tau = 0.6$ and $\mu = 0.6$, and the information span parameter is set to $\lambda = 0.2$; the effects of different load distribution strategies ($\alpha = 0.1$, $\beta = 0.9$; $\alpha = 0.3$, $\beta = 0.7$; $\alpha = 0.5$, $\beta = 0.5$; $\alpha = 0.7$, $\beta = 0.3$; $\alpha = 0.9$, $\beta = 0.1$) on network invulnerability under different information accuracies are shown in Figure 5.

As can be seen from Figure 5, under different information accuracies, the impact of load distribution strategies on the network invulnerability presents varied characteristics. According to Figures 5(a) and 5(c), when $\delta = 0$, 0.2, $\alpha = 0.5$, $\beta = 0.5$, the network invulnerability is optimal. But the network invulnerability is poor when $\alpha = 0.1$, $\beta = 0.9$ and $\alpha = 0.9$, $\beta = 0.1$. In other words, the more balanced weight of the spatial distance and the connected edge residual capacity is, the stronger the network invulnerability will be. According to Figure 5(d), when $\delta = 0.3$, the network invulnerability increases with the load distribution weighting the spatial distance weight.

As can be seen from the above, the methodology aims at the passenger evacuation for failed nodes in the urban agglomeration transportation network. When the attacker knows little about the network information, the evacuation strategy will reduce the impact of the cascading failures and make better invulnerability of transportation by considering the impact of the residual capacity and the spatial distance.

Moreover, when the attacker knows more about the network information, the evacuation strategy based on the distance of adjacent station will reduce the impact of the cascading failure and make better invulnerability of transportation.

5. Conclusions

This paper proposes the cascading failure model of the urban agglomeration passenger transport network based on the improved capacity-load model. A simulation scenario on the invulnerability of Hu-Bao-E-Yu urban agglomeration transportation network under incomplete information attack is built based on different node load factors and load distribution mechanisms. The research conclusions are as follows:

(1) The attack information span has a threshold 0.9, and the degree of information accuracy has a threshold 0.6. Once one of the thresholds is exceeded, maximum damage to the network can be achieved. Therefore, the attacker does not need to obtain all the information of the network, and the obtained information only needs to exceed a certain value to achieve the best attack effect.

(2) Under the influence of attackers' access information of the network, the site redundant capacity will be too high or too low, which will reduce the invulnerability of urban agglomeration transportation network. Therefore, larger station scale may not be beneficial to the improvement of invulnerability.

(3) Due to the large gap of different sites, the transportation network shows strong robustness to random attacks and vulnerability to deliberate attacks. A few key sites play a decisive role in the normal operation of the urban agglomeration transportation network.

(4) The impact of different load distribution strategies on network invulnerability is also different with the situation of the attackers' access network information. Therefore, to reduce the impact of cascading failure and improve the resilience of urban agglomeration transportation network, strategies with different weights of factors are considered to deal with various types of attackers.

The research in this article helps to further reveal the cascading failure mechanism of the urban agglomeration transportation network in reality. The article explores how different factors can resist the destruction of the urban agglomeration passenger transportation network when the attacker fails to fully grasp the network information to attack the network. The research results show that a small number of key sites have a decisive effect on whether the urban agglomeration traffic network can maintain good resilience. This reminds the urban agglomeration traffic management personnel to identify those more important sites that need daily special maintenance. In addition, when an accident causes some stations in the transportation network to fail, managers should formulate passenger flow evacuation strategies under different conditions to ensure the minimal impact on the network.

This paper constructs a passenger transportation network model for urban agglomerations based on complex networks. Then the survivability of the network is analyzed. In the process of constructing the network model, the composite method adopted and referred to the actual traffic network. However, there are not entirely the same in terms of dynamic characteristics. More specifically, in a composite network, the load of the network node is relatively fixed, while it is always changing in the realistic network. At the same time, in the process of cascade failure simulation, the evacuation of passengers cannot be carried out simultaneously due to the influence of time. In addition, the existing research mainly focuses on the dynamic simulation of the invulnerability characteristics of the urban agglomeration traffic network, and the related research on optimization and repair has not been carried out in depth, so further research will focus on the above issues.

Data Availability

The tabular data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The work presented in this paper was partially funded by the Special Fund of National Natural Science Foundation of China (Grant no. 71940010), General Fund of Natural Science of Inner Mongolia (Grant no. 2019MS05083), Research Program of Science and Technology at Universities of Inner Mongolia Autonomous Region (Grant no. NJZY19013), and the Young Scientists Fund of Natural Science of Inner Mongolia (Grant no. 2019BS07002).

References

[1] J. He, C. Li, Y. Yu, Y. Liu, and J. Huang, "Measuring urban spatial interaction in Wuhan urban agglomeration, Central China: a spatially explicit approach," *Sustainable Cities and Society*, vol. 32, pp. 569–583, 2017.

[2] X. S. Luo and B. Zhang, "Analysis of cascading failure in complex power networks under the load local preferential redistribution rule," *Physica A: Statistical Mechanics and its Applications*, vol. 391, no. 8, pp. 2771–2777, 2012.

[3] W. Ren, J. Wu, X. Zhang, R. Lai, and L. Chen, "A stochastic model of cascading failure dynamics in communication networks," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, no. 5, pp. 632–636, 2018.

[4] A. Plietzsch, P. Schultz, J. Heitzig, and J. Kurths, "Local vs. global redundancy-trade-offs between resilience against cascading failures and frequency stability," *The European Physical Journal Special Topics*, vol. 225, no. 3, pp. 551–568, 2016.

[5] R.-R. Yin, B. Liu, H.-R. Liu, and Y.-Q. Li, "Research on invulnerability of the random scale-free network against

cascading failure," *Physica A: Statistical Mechanics and its Applications*, vol. 444, pp. 458–465, 2016.

[6] H. J. Sun, H. Zhao, and J. J. Wu, "A robust matching model of capacity to defense cascading failure on complex networks," *Physica A: Statistical Mechanics and its Applications*, vol. 387, no. 25, pp. 6431–6435, 2008.

[7] J. Lehmann and J. Bernasconi, "Stochastic load-redistribution model for cascading failure propagation," *Physical Review E*, vol. 81, no. 3, Article ID 031129, 2010.

[8] W. X. Wang and G. Chen, "Universal robustness characteristic of weighted networks against cascading failure," *Physical Review E*, vol. 77, no. 2, Article ID 026101, 2008.

[9] H.-P. Ren, J. Song, R. Yang, M. S. Baptista, and C. Grebogi, "Cascade failure analysis of power grid using new load distribution law and node removal rule," *Physica A: Statistical Mechanics and its Applications*, vol. 442, pp. 239–251, 2016.

[10] M. Du, X. Jiang, L. Cheng et al., "Robust evaluation for transportation network capacity under demand uncertainty," *Journal of Advanced Transportation*, vol. 2017, Article ID 9814909, 11 pages, 2017.

[11] J. Wang, L. Rong, L. Zhang, and Z. Zhang, "Attack vulnerability of scale-free networks due to cascading failures," *Physica A: Statistical Mechanics and its Applications*, vol. 387, no. 26, pp. 6671–6678, 2008.

[12] L. Zhang, B.-b. Fu, and Y.-x. Li, "Cascading failure of urban weighted public transit network under single station happening emergency," *Procedia engineering*, vol. 137, pp. 259–266, 2016.

[13] F. Chaoqi, W. Ying, W. Xiaoyang, and G. Yangjun, "Multi-node attack strategy of complex networks due to cascading breakdown," *Chaos, Solitons & Fractals*, vol. 106, pp. 61–66, 2018.

[14] X. G. Tian and C. M. Zhang, "Survivability model of equipment support network based on incomplete information," *System Engineering-Theory & Practice*, vol. 37, no. 3, pp. 790–798, 2017.

[15] Z. Chen, W.-B. Du, X.-B. Cao, and X.-L. Zhou, "Cascading failure of interdependent networks with different coupling preference under targeted attack," *Chaos, Solitons & Fractals*, vol. 80, pp. 7–12, 2015.

[16] Y. Cai, Y. Cao, Y. Li, T. Huang, and B. Zhou, "Cascading failure analysis considering interaction between power grids and communication networks," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 530–538, 2016.

[17] S. Hong, B. Wang, X. Ma, J. Wang, and T. Zhao, "Failure cascade in interdependent network with traffic loads," *Journal of Physics A: Mathematical and Theoretical*, vol. 48, no. 48, p. 485101, 2015.

[18] J. J. Wu, H. J. Sun, and Z. Y. Gao, "Cascading failures on weighted urban traffic equilibrium networks," *Physica A: Statistical Mechanics and its Applications*, vol. 386, no. 1, pp. 407–413, 2007.

[19] Y. Yan, S. Zhang, J. Tang, and X. Wang, "Understanding characteristics in multivariate traffic flow time series from complex network structure," *Physica A: Statistical Mechanics and its Applications*, vol. 477, pp. 149–160, 2017.

[20] O. Cats and E. Jenelius, "Planning for the unexpected: the value of reserve capacity for public transport network robustness," *Transportation Research Part A: Policy and Practice*, vol. 81, pp. 47–61, 2015.

[21] 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.

[22] E. Jenelius and O. Cats, "The value of new public transport links for network robustness and redundancy," *Transportmetrica A: Transport Science*, vol. 11, no. 9, pp. 819–835, 2015.

[23] A. De-Los-Santos, G. Laporte, J. A. Mesa, and F. Perea, "Evaluating passenger robustness in a rail transit network," *Transportation Research Part C: Emerging Technologies*, vol. 20, no. 1, pp. 34–46, 2012.

[24] C. B. Li, L. Wei, and Y. C. Hao, "Research on characteristics of city agglomeration compound traffic network," *Journal of System Simulation*, vol. 28, no. 12, pp. 2958–2965, 2016.

[25] C. B. Li, L. Wei, F. X. Li et al., "Study on vulnerability of city agglomeration compound traffic network based on attack strategy," *Journal of Highway and Transportation Research and Development*, vol. 34, no. 3, pp. 101–109, 2017.