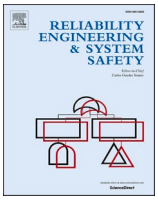
Reliability Engineering and System Safety 214 (2021) 107779

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress



Vulnerability analysis of road network for dangerous goods transportation considering intentional attack: Based on Cellular Automata

Wencheng Huang [a,b,c,d,*], Bowen Zhou [a,b], Yaocheng Yu [a,b], Dezhi Yin [a,b]

[a] School of Transportation and Logistics, Southwest Jiaotong University, Chengdu, Sichuan 611756, China
[b] Institute of System Science and Engineering, Southwest Jiaotong University, Chengdu, Sichuan 611756, China
[c] National United Engineering Laboratory of Intergrated and Intelligent Transportation, Southwest Jiaotong University, Chengdu, Sichuan 611756, China
[d] National Engineering Laboratory of Integrated Transportation Big Data Application Technology, Southwest Jiaotong University, Chengdu, Sichuan 611756, China

ARTICLE INFO

Keywords:
Road network for dangerous goods transportation
Vulnerability analysis
Cascading failure
Cellular Automata
Node recovery ability
Intentional attack

ABSTRACT

The vulnerability of road network for dangerous goods transportation (RNDGT) under cascading failure considering intentional attack is analyzed. We introduce the time characteristics of load distribution and node recovery ability into previous cascading failure model, subdivide the state of failed node into normal state, partial failure state and complete failure state. Six traffic load distribution strategies including Average Distribution (AD), Betweenness Distribution (BD), Capacity Distribution (CD), Degree Distribution (DD), Tightness Distribution (TD) and Surplus Load Distribution (SLD) are selected to study the load re-distribution of failed nodes. In addition, three kinds of intentional node attack strategies including Degree Attack (DA), Betweenness Attack (BA) and Tightness Attack (TA) are selected to study the impact on the vulnerability. By referring the application of cellular automata applied in epidemic spreading field, we establish a new cascading failure model of RNDGT. The improved maximum connectivity and node failure rate based on node degree are applied to analyze the vulnerability. A case study is conducted by using the RNDGT of Dalian as the background. The previous Motter-Lai model (M-L) is applied as the comparison approach. TA strategy has the least impact on increasing network vulnerability, SLD strategy is the best to reduce network vulnerability.

1. Introduction

With the continuous expansion of energy and chemical industry scale, the demand of dangerous goods continues increasing. Dangerous goods have some special characteristics, such as strong destructiveness and wide diffusion range, which are easy to cause secondary hazards. In addition, the production places and demand places of dangerous goods are generally distributed in different regions, the transportation process of dangerous goods is indispensable and road transportation is the main mode of dangerous goods transportation [36]. For example, in China, more than 60% of dangerous goods are transported by road. However, with the dangerous goods transportation volume increasing, the accidents of dangerous goods road transportation are also increasing year by year, e.g., from 2012 to 2016, there were 177, 387, 394, 406 and 496 road transport accidents of dangerous goods in China during each year, with 91, 194, 208, 217 and 280 deaths, respectively [28]. Once the road dangerous goods transportation accident occurs, it will not only bring great pressure to the relevant production management departments, but also cause adverse social impact. In recent years, the safety transportation of dangerous goods has become a common concern of the whole society.

Some previous works have been devoted to the road dangerous goods transportation related researches, e.g., Purdy [43] analyzed and compared the risk of the transportation of dangerous goods by road and rail, the results indicated that the safe routing of materials with large hazard ranges may be more easily achieved by road; From the technical and administrative factors perspective, Andersson [4] investigated and compared the dangerous goods transportation safety by rail and by road, as well as the safety by sea transport and by land transport; By using coupling coordination degree approach, Huang et al. [28] evaluated the risk in the road dangerous goods transport system; Conca et al. [12] analyzed the interactions between accidents frequency and road traffic flow, and established a model to solve the minimum cost routing problem for a road carrier considering the risk related to dangerous goods; Based on a dynamic model of conditional value-at-risk (CVaR) measure, Faghih-Roohi et al. [19] analyzed the risk assessment and

* Corresponding author at: School of Transportation and Logistics, Southwest Jiaotong University, Chengdu, Sichuan 611756, China.
E-mail address: 1261992248@qq.com (W. Huang).

https://doi.org/10.1016/j.ress.2021.107779
Received 29 December 2020; Received in revised form 11 April 2021; Accepted 6 May 2021
Available online 14 May 2021

mitigation of hazardous material transportation in supply chain networks; Benekos and Diamantidis [8] discussed and compared qualitative, semi-quantitative and quantitative approaches that applied in risk assessment of dangerous goods transportation through road tunnels in Greece; Based on risk analysis, Lundin and Antonsson [36] established a comprehensive and flexible approach for categorizing road tunnels according to regulations regarding transportation of dangerous goods (ADR); Bęczkowska [7] proposed an optimal route selection model of road dangerous goods transportation from the perspective of risk and losses minimization, and designed a Breadth First Search algorithm (BFS) to optimize the route; Niu and Ukkusuri [42] investigated the relationship between exposure factors and driving risk of commercial dangerous goods truck, a Weibull distribution based approach was proposed to evaluate the risk of specific transportation environment, e.g., specific transportation route; For a time-dependent urban road network with hazardous materials transportation, Chiou [10] proposed a resilience-based signal control approach to manage maximum risk over links; Zhang et al. [59] proposed a gravity-based model considering both network topology and risk characteristics to evaluate the vulnerability of a hazmat road transportation network.

As the conclusions, we can find that most of the previous works are related to risk evaluation, risk control, optimal route selection and vulnerability evaluation of dangerous goods transportation by road. Few works have been devoted to analyzing vulnerability of road network for dangerous goods transportation (RNDGT) under cascading failure considering intentional attack. Usually, vulnerability is defined as a weak link that may cause damage in the network/system. Vulnerability analysis refers to the process of finding out the weak points in the network/system, which is an important part of risk evaluation of the network/system. RNDGT is an important carrier of dangerous goods transportation process, and its stability and reliability are the prerequisite to ensure the safety of dangerous goods transportation. Some unpredictable internal or external factors will lead to the damage of dangerous goods transportation function, which will increase the vulnerability of dangerous goods road transportation network. In the RNDGT, the capacity of node is limited. Once traffic accident or terrorist attack occurred in the node, the load originally existing on the failed node will be distributed to other nodes or paths, and the load of each node will change accordingly due to the strong relevance of the network. However, the limited capacity of each node limits its load sharing ability, when the loads of these nodes exceed their own load capacity, the overload nodes will also fail, and then enter a new round of load distribution and node failure, circularly [6,22]. When the proportion of failed nodes in the network increases gradually, the failures spread through the network through coupling and linking, and finally leads to the collapse of the whole network [17,66], such dynamical phenomena in complex networks is the cascading failures [60,67]. The importance degree of different nodes in the network varies greatly, the failure of some nodes with high importance degree will affect the vulnerability of the whole network [1,2].

From safety management and operation of network/node perspective, how to evaluate the mutual influence of load redistribution among nodes when different nodes (or combination of nodes) fail, then explore the different impacts of different nodes on network vulnerability and finally effectively identify the vulnerable nodes of the network under different node attack strategies, are the main issues to ensure the safety and reliability of the RNDGT. Moreover, from emergency rescue perspective, providing better defense resources for key nodes and selecting more appropriate traffic load distribution strategies can reduce the damage of network cascading failure, to improve the survivability of network in sudden situation, and reduce the vulnerability of RNDGT. In this paper, we use Cellular Automata to analyze the vulnerability of RNDGT under cascading failure considering intentional attack, the failure transmission and the scale of failed nodes are also analyzed. The impacts of different intentional node attack strategies and different traffic load distribution strategies on vulnerability are discussed. We hope our works can provide some practical guidance for managers, planners and first responders.

The remainder of this paper is organized as follows. Section 2 is devoted to the literature review of vulnerability of network, and the Cellular Automata related works. Section 3 is devoted to the establishment of RNDGT and vulnerability analysis indicators. In Section 4, the intentional node attack strategies and traffic load distribution strategies in RNDGT are introduced. In Section 5, we introduce the vulnerability analysis processes of RNDGT under cascading failure based on Cellular Automata. Section 6 is devoted to the case study by using the RNDGT of Dalian, China as the background. In Section 7, the major conclusions and an outline of future research tasks are presented.

2. Literature review

This section is devoted to the literature review of vulnerability of network, and the literature review of Cellular Automata. The advantages and limitations will be discussed, the contributions of this paper will also be presented.

(i) The literature review of vulnerability of network

Vulnerability is a potential weak link in the system that may be attacked or used to cause damage to the system, which describes the characteristics of objects that are vulnerable to be attacked or damaged [37]. Initially, vulnerability is defined as the degree of disaster impact caused by unexpected events in the system [51]. In terms of traffic network analysis, the vulnerability is variously defined from different research perspectives and measurement indicators, e.g., Berdica [9] firstly gave the definition of road network vulnerability, which refers to the sensitive coefficient of sharp decline of road network service level caused by abnormal events, the sensitive coefficient is related to load capacity, transfer performance, travel time and other factors; D'Este and Taylor [14] considered that the road traffic network vulnerability focused more on the severity of the event consequences, the connectivity vulnerability between two nodes and the reachable vulnerability of a single node are defined, respectively; Husdal [29] thought that the vulnerability of road network belongs to risk, it is a certain characteristic that the road traffic network is not able to operate normally when some unexpected situations happened, which is related to the occurrence probability of external conditions or threats, and mainly emphasizes the consequences of road network vulnerability; Erath et al. [18] thought that the vulnerability of road network is the product of failure probability and failure consequence; Jenelius and Mattsson [31] defined the vulnerability of road network as the risk of social damage and degradation of transportation system, and considered that vulnerability is mainly related to the occurrence probability and the consequences of dangerous events in specific locations. There are two kinds of the research approaches on the vulnerability of transportation network, including static ergodic failure method and dynamic load distribution method [37]. Next, we introduce the two analysis approaches.

Static ergodic failure method, which selects a node or edge to be attacked (intentional attack or random attack) randomly each time, the static traffic load distribution results or network topology state are used to evaluate the impact of node or edge failure on the service capacity of the whole traffic network, so as to identify the vulnerable nodes or edges. For example, Scott et al. [45] considered the flow, capacity and topological structure of the road network, the travel time is used to identify the key links of the road network; Based on OD distribution matrix of road network, Jenelius et al. [30] used the difference of total travel cost after network edge failure to evaluate the impact of side failure on road network vulnerability; Ye [58] adopted the node degree, average path length, clustering coefficient etc. to study the vulnerability of rail transit stations under deliberate attack, and the key stations are identified by the global efficiency index of the network; Dong et al. [[15] a] considered the betweenness and traffic flow in the road network,

defined the importance of nodes and edges to identify the vulnerable sources of road network, and used the index of minimum cut degree vector to analyze the vulnerability of topological structure of urban road network; Based on the increase in generalized travel cost when links are closed, Jenelius et al. [30] derived link importance indices and site exposure indices, and applied these indices to evaluate the reliability and vulnerability of road network of northern Sweden; From the perspective of the delays imposed to disrupted airline passengers, Augusto et al. [5] analyzed the vulnerability of the European air transport network to major airport closures; Zhang et al. [[61]b] established a novel vulnerability assessment and visualization framework from a route service disruption perspective.

Dynamic load distribution method, which firstly selects nodes or edges randomly to fail, then dynamically redistributes the traffic load of the failure node or edge, and finally evaluates the impact of node or edge failure on the vulnerability of the whole traffic network. Under combining the cascading failure model, the dynamic load distribution method generally introduces time parameter into the static road traffic network model to describe the dynamic change process of network topology and other attributes [37]. For example, based on the user balance allocation model, Lei and Ba [34] constructed a cascading failure model for actual traffic networks, the index of Motter-Lai model (M-L) was used to evaluate the effectiveness of the global network or sub-network, and to measure the vulnerability of the road section in the network; Based on the connectivity loss of topological structure of water distribution networks, Shuang et al. [46] evaluated the nodal vulnerability under cascading failures with intentional attack; Zheng [64] comprehensively considered the changes of road network vulnerability and congestion degree in the cascading failure process caused by road congestion failure, and introduced congestion factor to evaluate road network vulnerability and congestion degree; Based on the user equilibrium assignment model and congestion propagation effect of road network, Dong et al. [[16]b] proposed a vulnerability assessment model considering the user travel time cost, energy and environmental cost, and used the failure consequences of road network units in road network to measure the vulnerability; Sun et al. [48] evaluated the key stations by considering node degree, betweenness and strength. Based on coupled map lattices, a model considering loading and redistribution of multi-static passenger flow was proposed to analyze the vulnerability under cascading failures of weighted rail transit network; Zhang and Yang [59] proposed a risk cascading propagation model to explore the vulnerability of interdependent research and development networks; Goodrum et al. [24] used network-based methods to reduce the design detail required for distributed system modeling and vulnerability analysis considering cascading failures; Lee and Hu [33] proposed a framework to model the smart grid as interdependent complex networks, investigated and compared the topology vulnerabilities under load redistribution attack and sequential attack according to the node importance; Hu and Fan [26] converted the complex grid into its dual graph, then ranked the vulnerability of transmission lines by using the M-Burt method, and devised a mitigation strategy against cascades considering the vulnerable transmission lines; Based on the thermal inertia-based cascades model combining an N-K contingency sampling algorithm, Yang et al. [57] analyzed the power system vulnerability in terms of its variable operation state and different generation uncertainty levels under cascades propagation.

As the conclusions, we can find that the previous researches on the vulnerability of transportation network mainly involve the definition of vulnerability, the construction of vulnerability evaluation index, and the identification of key nodes or sections. Although there are many definitions of network vulnerability, its core idea can be summarized as the consequence of network unit failure and the failure probability of network unit. In general, the failure probability is more difficult to quantify accurately than the failure consequence. The purpose of network vulnerability analysis is to identify the vulnerable links in the network, that is, to identify the sections or nodes that have significant impacts on the whole network under emergencies.

(i) **The literature review of Cellular Automata**

Cellular Automata (CA) model belongs to a kind of grid dynamic model with discrete space-time, discrete state, local change in time and spatial interaction, which can simulate the spatiotemporal evolution process of complex systems. Each independent cell element is finite and distributed discretely, starting from the local and evolving with certain rules. The CA is composed of a series of rules with cellular space, state set, cellular neighborhood and state transition rules, and without fixed physical equations or mathematical equations, any model that satisfies these rules can be regarded as CA model, therefore, CA is the general name of a kind of model or a method framework [3,55]. Nowadays, a lot of CA models have been developed and applied in many fields. Next, we conclude these works that applied in traffic and transportation field and in epidemic spreading field.

In traffic and transportation field. The classical traffic flow models based on CA include Rule 184, NS model, TT model and KKW model. Rule 184 was firstly proposed by Wolfram [54], which is the simplest and most basic CA traffic flow model. In Rule 184, the road is separated into several equidistant grids, where 0 indicates that the cell is empty, and 1 indicates that the cell is occupied by vehicles, the state transition rule describes the phase transition of free flow and congestion flow. Based on Rule 184, the NS model was proposed by Nagel and Schreckenberg [41], which considered stochastic slowing down rules, the differences of driver's behavior and the maximum speed, and described the actual traffic phenomena such as ghost traffic jam, time travel and stop wave etc. Based on NS model with single lane traffic flow, Xu et al. [56] studied the influence of relative motion between vehicles and deceleration probability on traffic state, the results show that in the process of vehicle movement, with the increase of vehicle density, its evolution is fluctuating. In addition, based on NS model, Ge et al. [23] introduced the variable safety distance to analyze the mixed traffic flow, the results show that the implementation of fast and slow traffic diversion can effectively expand the traffic flow and reduce the generation of congestion. Within a tolerance comparable with a single jam spacing, Daganzo [13] proved that the vehicle trajectories predicted by a simple linear car-following model, the kinematic wave model with a triangular fundamental diagram, and two cellular automata models CA (car-following model) and CA (kinematic wave model) match everywhere. TT model was firstly proposed by Takayasu and Takayasu [49], which improved NS model by considering density of vehicles, revealed the phase conversion between the blocking phase and the non-blocking phase. The random disturbance factors were introduced in TT model, the power spectrum 1/f in the interference phase and the white noise in the non-interference phase were observed. Kerner et al. [32] firstly proposed three-phase traffic theory and introduced the CA into microscopic traffic flow model, and developed the KKW model. Based on the interaction between vehicles in car following theory, the evolution rules of certainty and randomness are formulated, and the adjustment mechanism such as random acceleration and deceleration of vehicles is realized by synchronous distance. After that, a lot of works have been devoted to traffic related researches, here we list some of the latest works, e.g., Meng and Weng [38] develop an improved cellular automata (ICA) model for simulating heterogeneous traffic in work zone; Tian et al. [50] applied cellular automaton to simulate spatiotemporal patterns, phase transitions and concave growth pattern of oscillations in traffic flow; Ruan et al. [44] used an improved cellular automaton with axis information to simulate microscopic traffic; Hua et al. [27] applied cellular automata to study how the arrangement of three-dimensional facilities on a road affects driving behavior; Zhao et al. [62] used cellular automata to urban road traffic characteristics considering Internet of Vehicles and emergency vehicles; Zeng et al. [63] proposed a new average speed feedback strategy based on real-time information, and uses it to improve the modified comfortable driving

cellular automaton model.

In epidemic spreading field. Considering the difference of cellular states, cellular automata of infectious diseases can be classified into three types including SIS, SIR and SEIRS. Combined with Graph Theory, Fresnadillo et al. [20] established a SIS epidemic model based on cellular automata. The state of each cell in the model represents the percentage of susceptible and infected individuals in a specific time step, and the local transfer function is used to control these evolution processes. They found that if no control measures are taken, the overall density of the exposed and infected individuals changes near the positive equilibrium point. When the infected individuals are partially isolated, the virus die out at a relatively slow speed. When the infected individuals are completely isolated, the virus is extinct soon. After that, they considered the rectangular and hexagonal cells, as well as the three kinds of cellular neighborhoods including von Neumann, Moore and hexagonal Moore, compared the degree of virus infection in different neighborhood [21]; Wang and Jiang [52] proposed a new SIS propagation model considering the influence of propagation delay on the dynamic behavior of virus propagation in complex networks; Considering the interaction and feedback of node dynamics and network dynamics, Song et al. [47] proposed a virus propagation model in adaptive network based on cellular automata by constructing SIS propagation rules and reconnection rules. White et al. [53] proposed SIR virus infection model based on two-dimensional cellular automata. The birth rate and immigration rate are not considered in the model, that is, the total number of people remains unchanged. The connection factor, mobility factor and virulence factor of the virus are defined. They found that the spread degree of virus is related to the neighborhood type of cell. The larger the connection factor is, the faster the spread speed of virus is. The uniform distribution of population is also related to the spread degree of virus. Vaccination can effectively control the transmission speed of virus and reduce the number of infected people. Liu and Jin [35] considered the five states including health, exposure, infection, immunity and death in the process of disease transmission, and established the SEIRS model based on binary cellular automata. The effects of five parameters including exposure rate, infection rate, infection and immunity, immunity and health, infection and death on exposure density and infection density were analyzed. The characteristics of virus transmission and evolution were analyzed under the conditions of exposure and infection with isolation measures and without isolation measures, respectively. They found that, in the case of non-isolation, the virus continues to exist, while in the case of isolation, the virus decreases. When the immunity constant is lower than a certain threshold, the density sequence of exposure and infection fluctuates near the positive equilibrium point.

As the conclusions, we can find that the researches and applications of cellular automata have been devoted to various fields. In traffic field, the works focus on the simulation of microscopic traffic flow, which fully considered the acceleration and deceleration process of vehicles and the safe braking distance, and simulated the running state of vehicles in single lane and multi lanes situations. In the non-traffic field, the works focuses on the application from the macro-level, e.g., in the field of complex network, the works emphasized the impact when cell was attacked on the performance of the network.

(i) The limitations of previous works and the contributions in this paper

The previous works have the following limitations: (i) For the previous researches of network vulnerability, from the consequences of road network unit failure or the failure probability of road network unit perspective, most works considered the static/dynamic load flow characteristics of road traffic network and conducted qualitative and quantitative analysis on vulnerability of road network (e.g., [45,37]). Few works have been devoted to the vulnerability analysis of RNDGT under cascading failure considering intentional attack. (ii) For the previous researches of cascading failure, most of works assume that there are three kinds of node states in the network including normal state, pending state and failure state [39,11]. The nodes in the failure state are completely blocked without recovery ability in the simulation time. However, in the real road dangerous goods transport network, overloaded node does not necessarily lead to complete node failure, traffic congestion only reduces the operational efficiency of nodes to a certain extent. Therefore, the node state and node recovery capacity under different failure degrees should be considered. (iii) Most previous works applied random attack strategy or intentional attack strategy to study the overall performance of the network [58,46,33]. For the road transportation network, attacks based on descending node degree or node betweenness are often used to measure the overall invulnerability and vulnerability performance of the network [58,48,15]. As one of the important characteristic parameters of the network, the node compactness reflects the difficulty of the node to reach other nodes, the attack based on compactness can also be summarized as an intentional attack strategy. Therefore, we can explore the impact of different node attack strategies on the overall vulnerability performance of the network. (iv) For the previous researches of cascading failure, most works only discuss the network performance under the average load distribution of traffic volume [46,58]. In particular, the load assignment schemes are based on the step size, each simulation step carries out a complete load distribution for all affected nodes without considering the possible difference of distribution time among different nodes. For the RNDGT, when the cascading failure occurs, the load distribution strategy is complex and diverse. Therefore, it is necessary to further explore the impact of different load assignment strategies on the vulnerability performance. (v) Previous CA related works in traffic and transportation field focus on the simulation of micro traffic flow (e.g., [38,50,44]). In other fields, CA can be used to simulate the spread of infectious disease in different types of complex networks (e.g., [52,35]). Few works have been applied to the research of RNDGT.

In this paper, we focus on the node failure of road network under intentional node attack. We only study the failure consequences of road network nodes because the occurrence probabilities of emergencies are difficult to predict. When the nodes of the RNDGT are in abnormal state due to intentional node attack, the failure nodes cause cascading failures and impact the whole network, such impact degree is defined as the vulnerability of RNDGT. In this paper, we introduce the time characteristics of load distribution and node recovery ability into the previous cascading failure models, subdivide the state of failed node into normal state, partial failure state and complete failure state, refer the application of cellular automata applied in epidemic spreading field, establish a new cascading failure model of RNDGT, and explore the vulnerability of RNDGT under different intentional node attack strategies and different traffic load distribution strategies.

3. The establishment of RNDGT and vulnerability analysis indicators

Transportation network belongs to a kind of complex network in real world, which has been studied by a lot of scholars. The nodes and edges of RNDGT are selected from the existing road network, comparing with the existing road network, RNDGT has the following characteristics: (i) The RNDGT is planned and designed with minimum transportation risk, generally, the nodes and edges are far away from the areas with high population density, such as residence community, schools, water sources, government agencies. (ii) Generally, the scale of RNDGT is smaller than the that of existing road network in a city. (iii) The important nodes and edges of RNDGT have high defense ability to prevent cascading failures caused by various emergencies. (iv) When the road transportation accidents occur in the RNDGT, the emergency response speed is faster, the rescue timeliness is stronger, and the load evacuation mode is more effective. (v) The average aggregation coefficient of RNDGT is much lower than that of road traffic network. We assume that: (i) The

nodes and edges of RNDGT have the same attributes and levels. (ii) The RNDGT is an undirected graph without considering the direction of edges. (iii) The weight of edge is the actual distance of the edge, the RNDGT belongs to a weighted network. (iv) The intentional attack will have impact on the node of RNDGT. We assume that the intentional attack will have no impact on the dangerous goods themselves, there is no derivative accidents such as explosion and combustion of dangerous goods caused by the intentional attack. The RNDGT G can be formulated as:

$$G = (V, E, W) \tag{1}$$

Where $V = \{v_i, i = 1, 2, 3, \cdots, M\}$ is the set of nodes, M is the total number of nodes in G. $E = \{e_{ij}, i.j = 1,2,3,\cdots,M, i \neq j\}$ is the set of edges. $W = \{w_{ij}, i.j = 1,2,3,\cdots,M, i \neq j\}$ is the set of weight of edges, the distance of each edge is the weight value. In addition, we assume $F = \{f_i, i = 1,2,3,\cdots, M\}$ is the set of loads of nodes, $C = \{c_i, i = 1, 2, 3, \cdots, M\}$ is the set of capacities of nodes, t is the time that the node fails.

The commonly used analysis indicators of vulnerability include network efficiency, average aggregation coefficient, average shortest path, average scale of cascading failure, maximum connectivity, node failure rate, nodal and link weights, unweighted auxiliary nodes etc. [57,25]. Among them, maximum connectivity and node failure rate are the most widely used indicators with simple calculation steps, which effectively avoid the problems of inaccurate analysis result caused by incomplete data collection of other indicators. However, in real-world network, it is unreasonable to use the number of failed nodes to represent the number of complete failed nodes and partial failed nodes. In order to distinguish the influence of complete failed nodes and partial failed nodes on the network performance, the improved maximum connectivity $\varphi_G(t)$ and node failure rate based on node degree $\mu_G(t)$ are developed and selected as the vulnerability analysis indicators of RNDGT:

$$\varphi_G(t) = \frac{1}{M}\left\{\sum_{i\in V_1} x_i + \sum_{i\in V_2}\left[1 - \frac{f_i(t) - c_i(t_0)}{\theta_i(t)c_i(t_0) - c_i(t_0)}\right]\right\} \tag{2}$$

$$\mu_G(t) = \frac{\sum_{i\in V_2} d_i^2(t)\varepsilon_i(t) + \sum_{i\in V_3} d_i^3(t)}{\sum_{i\in V} d_i(t_0)} \tag{3}$$

Where V_1 is the set of normal nodes at time t, V_2 is the set of partial failed nodes at time t, V_3 is the set of complete failed nodes at time t, and $V_1 \cup V_2 \cup V_3 = V$, $x_i = 1$. $f_i(t)$ is the load of partial failed node at time t, $c_i(t_0)$ is the initial capacity of partial failed node at initial time t_0, $t > t_0$, $\theta_i(t)$ is the failure coefficient of partial failed node at time t. $d_i^2(t)$ is the degree of partial failed node at time t, $d_i^3(t)$ is the degree of complete failed node at time t, $d_i(t_0)$ is the node degree at initial time t_0, $\varepsilon_i(t)$ is the failure degree of partial failed node at time t. The node degree is the number of edges directly connected to the node.

Based on the load and capacity of each node, and the network topology of RNDGT, we can establish the cascading failure model based on cellular automata, compare the improved maximum connectivity $\varphi_G(t)$ and node failure rate based on node degree $\mu_G(t)$ under different traffic load distribution strategies, compare and analyze the impacts of different settings of failure coefficient $\theta_i(t)$ and recovery rate $\delta_i(t)$ on the vulnerability, and compare and analyze the impacts of different attack strategies on the vulnerability.

4. The node attack strategies and traffic load distribution strategies in RNDGT

The capacity of each node in the RNDGT is limited, when the load of the node exceeds the upper limit of its capacity, the node is in congestion state. When a node fails, the load that should pass through the failed node will follow the pre-set traffic load distribution strategy and evacuate to the connected nodes. Once these connected nodes get extra load and exceed their capacity limit, the nodes will also fail. Therefore, the mismatching between node capacity and traffic load volume is the main reason for cascading failure of RNDGT. The key factors of cascading failure in RNDGT include node attack strategies, traffic load distribution strategies and state transition rules, the state transition rules based on CA will be introduced in Section 5, here we introduce the node attack strategies and traffic load distribution strategies applied in this paper.

Node attack strategies. Random attack and intentional attack are the main attack methods. Random attack refers to that the saboteurs do not know all the information of the RNDGT, and attack the nodes or edges of the network randomly under ignoring the importance of nodes or edges. While intentional attack refers to that the saboteurs know all the information of the RNDGT, understand the importance and spatial position of nodes and edges, and attack the key nodes or edges in the network deliberately. The intentional attack includes ascending attack and descending attack based on the node degree or based on the betweenness. In this paper, we focus on the intentional attack and descending attack. More specifically, we select and compare the node attack strategies of the nodes include Degree Attack (DA), Betweenness Attack (BA) and Tightness Attack (TA), the nodes with higher node degree, betweenness or compactness are selected to attack each time.

Traffic load distribution strategies. The transport of dangerous goods by road is based on an Origin-Destination (OD) matrix that represents the transport demand over time. In this paper, we think the demand of dangerous goods by road will remain unchanged in a short time after the attack occurred, which means the transportation demand is rigid, and the traffic flows also remain unchanged. Hence, the traffic load distribution strategies are necessary. In this paper, we choose Average Distribution (AD), Betweenness Distribution (BD), Capacity Distribution (CD), Degree Distribution (DD), Tightness Distribution (TD) and Surplus Load Distribution (SLD) to study the load re-distribution of failed nodes.

(i) AD strategy. When the node i fails at time t, the traffic load percolates to the neighbor nodes. Assume that there are $N_i(t)$ normal neighbor nodes when i fails at time t, then the distribution ratio of traffic load $\Pi_{AD}^{i\to j}$ from failed node i to normal neighbor node j is:

$$\Pi_{AD}^{i\to j} = 1 / N_i(t) \tag{4}$$

(ii) **BD strategy**. The betweenness reflects the importance of node in the network. If the number of shortest paths between node i and node i', $i \neq i'$ is $S_{i\to i'}$, among them, the number of shortest paths that pass through node j is $S_{i\to i'}^j$, then the betweenness of node j is the proportion of the number of shortest paths passing through node j to the total number of shortest paths in the network. The greater the betweenness, the higher the node importance. Assume that the betweenness of neighbor node j when i fails at time t is $B_j(t)$, then the distribution ratio of traffic load $\Pi_{BD}^{i\to j}$ from failed node i to normal neighbor node j is:

$$\Pi_{BD}^{i\to j} = B_j(t) \Big/ \sum_j B_j(t) \tag{5}$$

$$B_j(t) = \sum_{i,i'} \left(S_{i\to i'}^j / S_{i\to i'}\right) \tag{6}$$

(iii) CD strategy. Once the intentional attack occurred, nodes with large capacity in the RNDGT will undertake more evacuation of traffic load. Assume that the capacity of neighbor node j when i fails at time t is $c_j(t)$, then the distribution ratio of traffic load $\Pi_{CD}^{i\to j}$ from failed node i to normal neighbor node j is:

$$\Pi_{CD}^{i\to j} = c_j(t) \Big/ \sum_j c_j(t) \tag{7}$$

(iv) DD strategy. The node degree reflects the number of edges connected to the node, so the larger the node degree, the more load it distributes. Assume that the degree of neighbor node$j$when$i$fails at time$t$is$d_j(t)$, then the distribution ratio of traffic load$\Pi_{DD}^{i\to j}$from failed node$i$to normal neighbor node$j$is:

$$\Pi_{DD}^{i\to j} = d_j(t) \Big/ \sum_j d_j(t) \tag{8}$$

(v) TD strategy. The tightness reflects the difficulty of node to reach other nodes, which is the reciprocal of the sum of distance$w_{jj'}$(the weight) from node$j$to all other nodes in the network. The higher the tightness is, the easier the node to reach other nodes, the load is easier to evacuate. Assume that the tightness of neighbor node$j$-when$i$fails at time$t$is$TD_j(t)$, then the distribution ratio of traffic load$\Pi_{TD}^{i\to j}$from failed node$i$to normal neighbor node$j$is:

$$\Pi_{DD}^{i\to j} = TD_j(t) \Big/ \sum_j TD_j(t) \tag{8}$$

$$TD_j(t) = 1 \Big/ \sum_{j'} w_{jj'}, j' \in V, j \neq j' \tag{9}$$

(vi) SLD strategy. In the process of node failure transfer, the larger the surplus load of the node, the more load it can undertake. The distribution ratio of traffic load$\Pi_{SLD}^{i\to j}$from failed node$i$to normal neighbor node$j$is:

$$\Pi_{SLD}^{i\to j} = \left[c_j(t_0) - f_j(t)\right] \Big/ \sum_j \left[c_j(t_0) - f_j(t)\right] \tag{10}$$

5. The vulnerability analysis processes of RNDGT under cascading failure based on cellular automata

As we have mentioned in Section 2, CA has been applied in epidemic spreading fields. We find some similarities between virus propagation process and cascading failure of nodes in RNDGT: (i) From the node characteristics perspective, in the epidemic spreading models based on CA, the individual (node) has a certain immune capacity, the immune capacity of the infected individual can defense the destruction of the virus. Only when the infection degree of the individual is greater than the individual immune capacity, the virus will successfully infect the individual and continue to spread to its contacts through the infected individual. In the RNDGT, the capacity of the node is limited, when the load of the node is greater than its capacity limit, the node might have failures and the load of the failed node might be further distributed to its neighbor nodes. (ii) In the epidemic spreading models based on CA, the infected individual's immune function will constantly attack the virus, so that the infected individual has a certain recovery ability. In the RNDGT, the failed node also has a certain node recovery ability, that is, the failure can be continuously alleviated by redistributing the load to its neighbor nodes. Next, we introduce the vulnerability analysis processes of RNDGT under cascading failure based on Cellular Automata. A Cellular Automata can be formulated by:

$$CA = \left(V, Q, \overline{V}, K\right) \tag{11}$$

Where$V$shows the Cellular Space, in this paper it is the set of nodes of RNDGT.$Q$is the set of cellular state, a cell only corresponds to one state at a certain time, the states of all cells at all discrete times form the set of cellular state. $\overline{V}$is the set of cell neighborhood, which represents the set of all neighbor nodes of any cell in the RNDGT.$K$is the state transition rules. Next, we introduce these elements of CA in the RNDGT.

(i) Cellular Space$V$

In this paper the nodes of RNDGT form the cellular space. Each node has initial load, node capacity and failure coefficient. The following initial load function considering time is applied to formulate the initial load of node:

$$f_i(t_o) = \left[d_i(t_0)\sum_{j\in\overline{V}_i} d_j(t_0)\right]^{\alpha}, i \neq j \tag{12}$$

Where$\overline{V}_i$is the set of cell neighborhood of node$i$,$f_i(t_o)$is the initial load of node$i$at initial timet_0,$d_i(t_0)$is the node degree of node$i$at initial timet_0,$d_j(t_0)$is the node degree of cell neighborhood node$j$.$\alpha$is the adjustable parameter of load, which controls the uniformity of initial load distribution in the RNDGT. According to the Motter-Lai model (M-L) [40], the node capacity in the RNDGT is proportional to the initial load:

$$c_i(t_0) = (1+\beta_i)f_i(t_o) \tag{13}$$

Where$c_i(t_0)$is the initial node capacity,β_i, $\beta_i > 0$is the tolerance coefficient of node$i$, which shows the ability of node$i$to handle additional load.$\theta_i(t)c_i(t_0)$in Eq.(2) shows the affordable maximum load of node$i$,$\theta_i(t), \theta_i(t) > 1$in Eq.(2) shows the failure coefficient.

(ii) The set of cellular state$Q$

The state of a node in the RNDGT has three possible states: normal, partial failure and complete failure. The cellular state$Q_i(t)$of node$i$can be formulated as:

$$Q_i(t) = \begin{cases} 0, i \in V_1 \\ (0,1), i \in V_2 \\ 1, i \in V_3 \end{cases} \tag{13}$$

(iii) The set of cell neighborhood$\overline{V}$

We use the adjacency matrix$\mathbf{A}_i^t$to represent the relationships among the node$i$and its neighbor nodes in set$\overline{V}_i$at time$t$, if the node$i$connects with node$j$,$j \in \overline{V}_i$, then we use$x_{i\leftrightarrow j} = 1$to represent the connection, and:

$$\overline{V}_i = \left\langle j \middle| j x_{i\leftrightarrow j} \in \mathbf{A}_i^t, x_{i\leftrightarrow j} = 1 x_{i\leftrightarrow j} \in \mathbf{A}_i^t, x_{i\leftrightarrow j} = 1 \right\rangle, i \neq j, x_{i\leftrightarrow i} = 0, x_{j\leftrightarrow j} = 0 \tag{14}$$

(iv) State transition rules$K$

The state transition rules in this paper include node state transition rules, dynamic traffic load distribution probability rules and time processing rules.

Node state transition rules. The state$Q_i(t+\Delta t)$of node$i$at time$t+\Delta t$is determined by its state$Q_i(t)$at time$t$and the state of its neighbor node$Q_j(t), j \in \overline{V}_i$in set$\overline{V}_i$at time$t$:

$$Q_i(t+\Delta t) = \begin{cases} \overline{\lfloor Q_i(t) \rfloor}, g_i(t) = 1 \\ \dfrac{f_i(t+\Delta t) - c_i(t_0)}{\theta_i(t)c_i(t_0) - c_i(t_0)}, g_i(t) \in (0,1) \\ \lfloor Q_i(t) \rfloor, g_i(t) = 0 \end{cases} \tag{15}$$

$$g_i(t) = \overline{\lfloor Q_i(t) \rfloor}\varepsilon_i(t) + \lfloor Q_i(t) \rfloor \delta_i(t) \tag{16}$$

Where $\overline{\lfloor Q_i(t) \rfloor}$ shows the reverse operation. $\lfloor\rfloor$ shows the round down operation. $g_i(t)$ is the state transition judgment function, when $g_i(t) = 0$, the state of node i is the same at both time $t + \Delta t$ and time t. $\delta_i(t), \delta_i(t) \in (0, 1)$ is the recovery rate of node i, which represents the recovery ability of node i. $f_i(t + \Delta t)$ is the load of node i at time $t + \Delta t$. $\theta_i(t)$ is the failure coefficient of partial failed node at time t, $\varepsilon_i(t)$ is the failure degree of partial failed node at time t, see Eq.(2). Based on Eqs.(15) and (16), we can find that:

When node i is in normal state at time t, then $Q_i(t) = 0, \lfloor Q_i(t) \rfloor = 0, \overline{\lfloor Q_i(t) \rfloor} = 1$, and $g_i(t) = \varepsilon_i(t)$. If $f_i(t + \Delta t) \le c_i(t_0)$, then $g_i(t) = \varepsilon_i(t) = 0, Q_i(t + \Delta t) = \lfloor Q_i(t) \rfloor$, the node will remain normal. If $c_i(t_0) < f_i(t + \Delta t) < \theta_i(t) c_i(t_0)$, the node state will be partial failure at time $t + \Delta t$, $g_i(t) = \varepsilon_i(t) = \lceil f_i(t + \Delta t) - c_i(t_0) \rceil / \lceil \theta_i(t) c_i(t_0) - c_i(t_0) \rceil = Q_i(t + 1)$. If $f_i(t + \Delta t) \ge \theta_i(t) c_i(t_0)$, then $g_i(t) = \varepsilon_i(t) = 1, Q_i(t + \Delta t) = \overline{\lfloor Q_i(t) \rfloor}$, the node state will be complete failure at time $t + \Delta t$.

When node i is in partial failure state at time t, then $Q_i(t) = \lceil f_i(t) - c_i(t_0) \rceil / \lceil \theta_i(t) c_i(t_0) - c_i(t_0) \rceil, \lfloor Q_i(t) \rfloor = 0, \overline{\lfloor Q_i(t) \rfloor} = 1$, and $g_i(t) = \varepsilon_i(t)$. The rules are the same with rules when node i is in normal state at time t.

When node i is in complete failure state at time t, $Q_i(t) = 1, \lfloor Q_i(t) \rfloor = 1, \overline{\lfloor Q_i(t) \rfloor} = 0$, and $g_i(t) = \delta_i(t). 0 < g_i(t) = \delta_i(t) < 1$, then $0 < g_i(t) = \delta_i(t) = \lceil f_i(t + \Delta t) - c_i(t_0) \rceil / \lceil \theta_i(t) c_i(t_0) - c_i(t_0) \rceil = Q_i(t + \Delta t) < 1$, the node state will be partial failure at time $t + \Delta t$.

Dynamic traffic load distribution probability rules. When the load of node is greater than its capacity, the node is not completely failed but the operation efficiency reducing. When the load of node is effectively evacuated, the network will return to normal. For the node in normal state, there is no load need to be evacuated. When the initial node i is totally failed by intentional attack at time t, its load will be totally distributed to its neighbor nodes at time $t + \Delta t_1$, for the neighbor node j, $j \in \overline{V}_i$, the load at time $t + \Delta t_1$ should be:

$$f_j(t + \Delta t_1) = f_j(t) + f_i(t)\Pi^{i\to j}, \Pi^{i\to j} \in \left\{\Pi_{AD}^{i\to j}, \Pi_{BD}^{i\to j}, \Pi_{CD}^{i\to j}, \Pi_{DD}^{i\to j}, \Pi_{TD}^{i\to j}, \Pi_{SLD}^{i\to j}\right\} \tag{17}$$

If $f_j(t + \Delta t_1) \le c_j(t + \Delta t_1)$, then $Q_j(t + \Delta t_1) = 0$, the node is normal and there is no load need to be evacuated. If $c_j(t + \Delta t_1) < f_j(t + \Delta t_1) < \theta_j(t + \Delta t_1) c_j(t + \Delta t_1), 0 < Q_j(t + \Delta t_1) < 1$, the node j is in partial failure state, we use dynamic traffic load distribution probability $P_j(t + \Delta t_1)$ to formulate the congestion degree of node j at time $t + \Delta t_1$:

$$P_j(t + \Delta t_1) = \left[\frac{f_j(t) - c_j(t_0)}{\theta_i(t) c_j(t_0) - c_j(t_0)}\right]^{\varpi} \tag{18}$$

Where ϖ, $\varpi \ge 1$ is the distribution coefficient. Then, the load of node j will carry at time $t + \Delta t_2, t + \Delta t_2 > t + \Delta t_1$ is presented in Eq.(19). Assume the set of neighbor nodes of node j is $\overline{V}_j$, for each node $k, k \in \overline{V}_j$, the load is presented in Eq.(20):

$$f_j(t + \Delta t_2) = P_j(t + \Delta t_1) f_j(t + \Delta t_1) \tag{19}$$

$$f_k(t + \Delta t_2) = f_k(t + \Delta t_1) + \left[1 - P_j(t + \Delta t_1)\right] f_j(t + \Delta t_1)\Pi^{j\to k}, \Pi^{j\to k} \in \left\{\Pi_{AD}^{j\to k}, \Pi_{BD}^{j\to k}, \Pi_{CD}^{j\to k}, \Pi_{DD}^{j\to k}, \Pi_{TD}^{j\to k}, \Pi_{SLD}^{j\to k}\right\} \tag{20}$$

If $f_j(t + \Delta t_1) \ge \theta_j(t + \Delta t_1) c_j(t + \Delta t_1), Q_j(t + \Delta t_1) = 1$, the node j is in complete failure state. Due to the recovery rate $r_j(t + \Delta t_1)$ of node j at time $t + \Delta t_1$, the complete failure state of node j at time $t + \Delta t_2$ will turn into partial failure state. Then, the load of node j will carry at time $t + \Delta t_2$ is presented in Eq.(21). Assume the set of s is $\overline{V}_j$, for each neighbor node $k, k \in \overline{V}_j$ of node j, the load is presented in Eq.(22). From initial time t_0, to initial node failure time t, to the first traffic load distribution time $t + \Delta t_1$ and the second traffic load distribution time $t + \Delta t_2$ etc., we can find out the obvious cascading failure transmission processes.

$$f_j(t + \Delta t_2) = c_j(t_0) + \left[\theta_j(t_0) c_j(t_0) - c_j(t_0)\right] \times \left[1 - r_j(t + \Delta t_1)\right] \tag{21}$$

$$f_k(t + \Delta t_2) = f_k(t + \Delta t_1) + \left[f_j(t + \Delta t_1) - f_j(t + \Delta t_2)\right]\Pi^{j\to k}, \Pi^{j\to k} \in \left\{\Pi_{AD}^{j\to k}, \Pi_{BD}^{j\to k}, \Pi_{CD}^{j\to k}, \Pi_{DD}^{j\to k}, \Pi_{TD}^{j\to k}, \Pi_{SLD}^{j\to k}\right\} \tag{22}$$

Time processing rules. In the previous cascading failure models, when a node fails suddenly at a certain time, the traffic loads of all the neighboring nodes should be recalculated in the next traffic load iteration. In the actual practice of RNDGT, the neighbor nodes of the failed node are not affected and redistribute the load at the same time, because the distances between the different neighbor nodes and the failed node are different from each other. In this paper, we assume the traffic distribution speed $\overline{v}$ is the same for all nodes. When initializing the network, the distance between node i and node j in the whole network is D_{ij}, the shortest path between the two nodes is $D_{ij}^{\min} = \min\{D_{ij}, i, j \in V, j \in \overline{V}_i\}$, then the minimum traffic load distribution time is $T_{ij}^{\min} = D_{ij}^{\min} / \overline{v}$. When the node i fails at time t, and the traffic loads of the neighbor nodes change at time $t + \Delta t_1$, then $\Delta t_1 = \min\{T_{ij}^{\min}, \forall j \in \overline{V}_i\}$. Calculate the traffic load and judge the state of node j at time $t + \Delta t_1$: If $Q_j(t + \Delta t_1) = 0$, the node j remains normal, the time interval between $t + \Delta t_2$ and $t + \Delta t_1$ should be $\min\{T_{ij'}^{\min} - T_{ij}^{\min}, \forall j, j' \in \overline{V}_i, j \ne j'\}$. If $Q_j(t + \Delta t_1) \ne 0$, the load of node j should be redistributed, the time interval between $t + \Delta t_2$ and $t + \Delta t_1$ should be $\min\{T_{ij'}^{\min} - T_{ij}^{\min}, T_{jk}^{\min}, \forall j, j' \in \overline{V}_i, j \ne j', k \in \overline{V}_j\}$. Repeat the steps until the transmission of cascading failure ends in the RNDGT.

The inputs of the simulation should be: the adjacency matrix $\mathbf{A}_i^t$, the adjustable parameter of load α, the tolerance coefficient of node β_i, the failure coefficient $\theta_i(t)$, the recovery rate $\delta_i(t)$, the distribution coefficient ϖ, the network G, the set of loads of nodes $F = \{f_i, i = 1,2,3,\cdots,M\}$, the set of capacities of nodes $C = \{c_i, i = 1,2,3,\cdots,M\}$. The outputs are the improved maximum connectivity $\varphi_G(t)$(Eq.2) and node failure rate based on node degree $\mu_G(t)$(Eq.3). The detail simulation steps are presented as follows:

Step 1: Generate RNDGT based on cellular automata, including the set of nodes $V = \{v_i, i = 1,2,3,\cdots,M\}$, the set of edges $E = \{e_{ij}, i.j = 1,2,3,\cdots,M, i \ne j\}$, the set of weight of edges $W = \{w_{ij}, i, j = 1,2,3,\cdots,M, i \ne j\}$, the adjacency matrix $\mathbf{A}_i^t, \forall i$.

Step 2: Calculate the node degree $d_i(t_0), \forall i$, betweenness of node $B_i(t_0), \forall i$ based on Eq.(6) and tightness node $TD_i(t_0), \forall i$ based on Eq.(9).

Step 3: Initialize the load and capacity of each node based on Eq.(12) and Eq.(13), respectively. Initialize the set of loads of nodes $F = \{f_i, i = 1,2,3,\cdots,M\}$, the set of capacities of nodes $C = \{c_i, i = 1,2,3,\cdots,M\}$.

Step 4: Select initial failure nodes. Assume that these nodes are attacked intentionally, the node attack strategies of the nodes include Degree Attack (DA), Betweenness Attack (BA) and Tightness Attack (TA). Assume there is no recovery ability of these nodes, remove them from the network, and update the set of normal nodes V_1, the set of partial failed nodes V_2 and the set of complete failed nodes V_3.

Step 5: Redistribute the traffic load. When the initial node i is totally failed at time t, its load (Eq.12) will be totally distributed to its neighbor nodes at time $t + \Delta t_1$, for the neighbor node $j, j \in \overline{V}_i$, the load distribution at time $t + \Delta t_1$ should follow Eq.(17).

Step 6: Update the information of the network. Update the node state $Q_i(t + \Delta t_1), \forall i \in V$. Update the adjacency matrix $\mathbf{A}_i^{t+\Delta t_1}, \forall i$. Record and update the nodes in the set of normal nodes V_1, the set of partial failed nodes V_2 and the set of complete failed nodes V_3, respectively.

Step 7: Judge the status of each node after load redistribution, update the load distribution and calculate load of each node $f_j(t + \Delta t_2)$ at time $t + \Delta t_2$. If $f_j(t + \Delta t_1) \le c_j(t + \Delta t_1)$, then $Q_j(t + \Delta t_1) = 0$. The node is normal and there is no load need to be evacuated, $f_j(t + \Delta t_1) = f_j(t + \Delta t_2)$ and turn to **Step 8**. If $c_j(t + \Delta t_1) < f_j(t + \Delta t_1) < \theta_j(t + \Delta t_1) c_j(t + \Delta t_1), 0 < Q_j(t + \Delta t_1) < 1$, the node j is in

partial failure state, put the node intoV_2, the load redistribution should follow Eq.(18), Eq.(19) and Eq.(20), and turn to **Step 6**. If$f_j(t+\Delta t_1) \geq \theta_j(t+\Delta t_1)c_j(t+\Delta t_1)$,$Q_j(t+\Delta t_1)=1$, the node$j$is in complete failure state, put the node intoV_3, the load redistribution should follow Eq.(21) and Eq.(22), and turn to **Step 6**.

Step 8: For each node$j$, if$Q_j(t+\Delta t_1)=0$, then the transmission process of node cascading failure ends after the attacks occur, and the network reaches a new equilibrium state.

Step 9: Output$\varphi_G(t)$(Eq.2) and$\mu_G(t)$(Eq.3), analyze the impact of cascading failures on the vulnerability of RNDGT. The detail simulation flowchart is presented in Fig. 1.

6. Case study

A case study is conducted by using the RNDGT and the transportation volume of Dalian, China as the background. There are 154 nodes and 238 edges of Dalian's RNDGT, and the transportation volume of each node is collected in September 2020, the load and capacity of each node will not present because of huge scale. Using Arc-GIS 10.2 to process the road network map of Dalian, the processes are presented in Fig. 2, the nodes in the network are the intersection of paths. The final network topology of RNDGT with node number of Dalian is shown in Fig. 2.

Based on Fig. 2, we can find that the number of nodes in the RNDGT is 154, the number of edges is 238. In addition, we can also calculate the characteristic parameters and analyze the structure of the RNDGT. These characteristic parameters include average node degree of network $< k >$, average path length L, average clustering coefficient of network$C$, the results are: $< k >= 3.0909$,$L = 64.4485$and$C = 0.1714$. $< k >= 3.0909$ means the average number of edges linked by each node is about 3, $L = 64.4485$ means the average length of any two nodes in the whole network is 64.4485 kms. As the comparison, we calculate the average path length$L_R$and average clustering coefficient of network $C_R$of a random network which has the similar size of RNDGT in Dalian, the results are: $L_R = 4.1871$and$C_R = 0.0216$. Because$L = 64.4485 \gg L_R = 4.1871$ and $C = 0.1714 \gg C_R = 0.0216$, hence, we can proof that the RNDGT of Dalian belongs to a small-world network.

Based on the load and capacity of each node, and the network topology of RNDGT in Dalian, we conduct the following works: (i) By using the previous M-L cascading failure model [40] and the cellular automata cascading failure model proposed in this paper, we compare the improved maximum connectivity$\varphi_G(t)$and node failure rate based on node degree$\mu_G(t)$under different traffic load distribution strategies (including AD, BD, CD, DD, TD and SLD). (ii) The impacts of different settings of failure coefficient$\theta_i(t)$and recovery rate$\delta_i(t)$on the vulnerability are compared and analyzed, respectively. (iii) The impacts of different attack strategies (including DA, BA and TA) on the vulnerability are compared and analyzed, respectively. The optimal traffic load distribution strategy under different attack strategies is given.

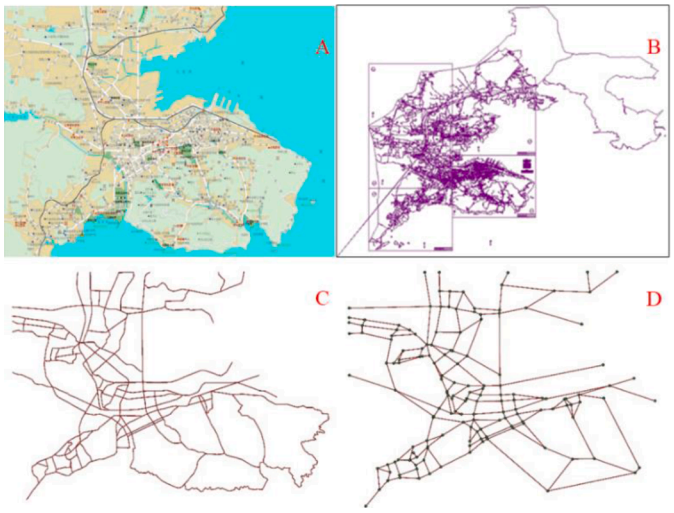


Fig. 2. The network processing based on Arc-GIS.

(i) The comparisons between M-L model and CA model under different traffic load distribution strategies

For the two cascading failure models, we select nodes with number 28, 32, 76, 84 and 54 as the initial failed nodes (see Fig. 3). For all nodes, the adjustable parameter of load$\alpha = 1$, the tolerance coefficient of node$\beta_i = 0.1$, the failure coefficient$\theta_i(t) = 1.1$, the recovery rate$\delta_i(t) = 0.1$, the distribution coefficient$\varpi = 1$. The$\varphi_G(t)$and$\mu_G(t)$under different traffic load distribution strategies based on M-L model is presented in Fig. 4. The$\varphi_G(t)$and$\mu_G(t)$under different traffic load distribution strategies based on CA model is presented in Fig. 5.

From the results in Fig. 4 and Fig. 5, we can obtain the following results: (i) For M-L model, when other parameters remain unchanged, the$\varphi_G(t)$decreases and tends to be stable with the increase of the number of iterations, while the$\mu_G(t)$increases and tends to be stable with the increase of the number of iterations. When the number of iterations is over 35, the vulnerability of RNDGT in Dalian remain unchanged. For the CA model, when other parameters remain unchanged,

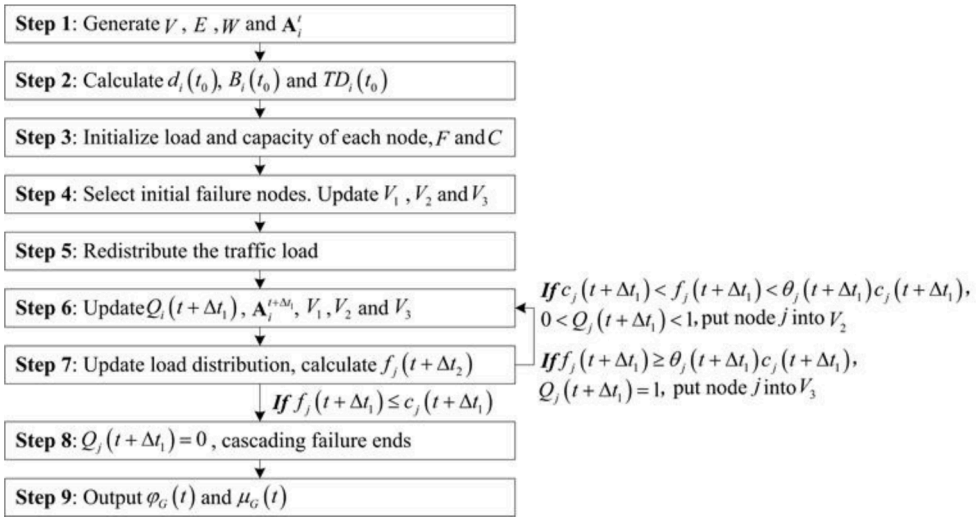


Fig. 1. The simulation flowchart.

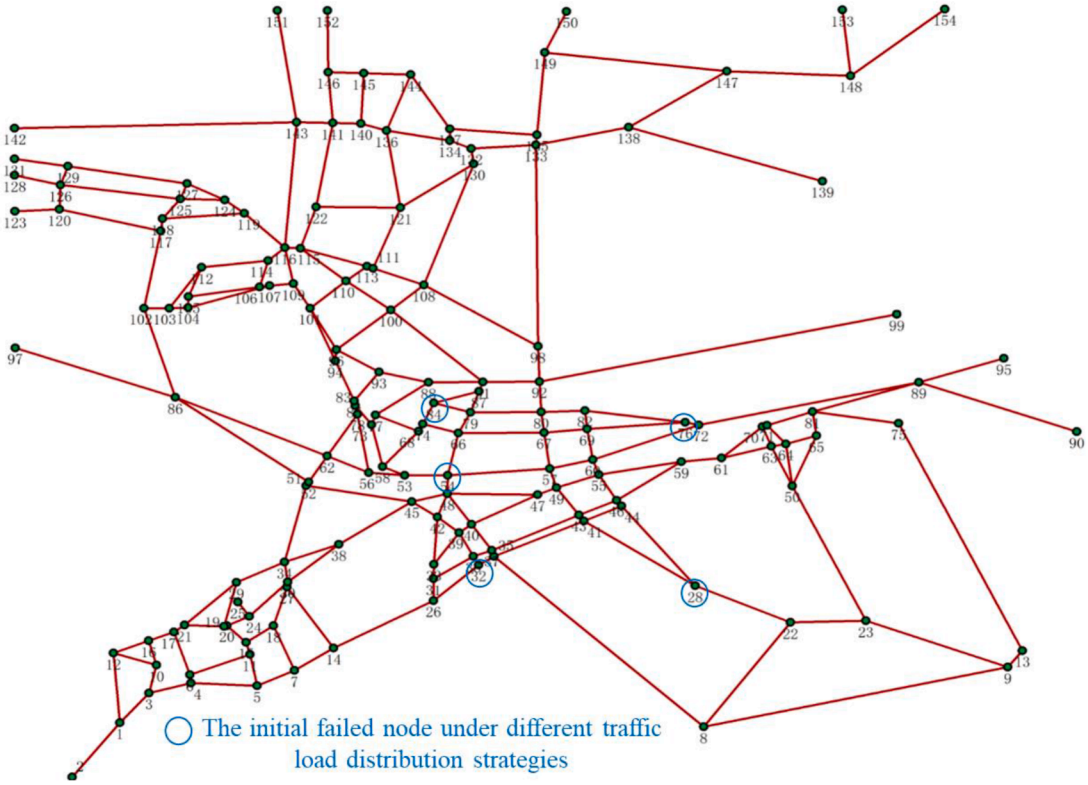


Fig. 3. The network topology with node number of RNDGT in Dalian.

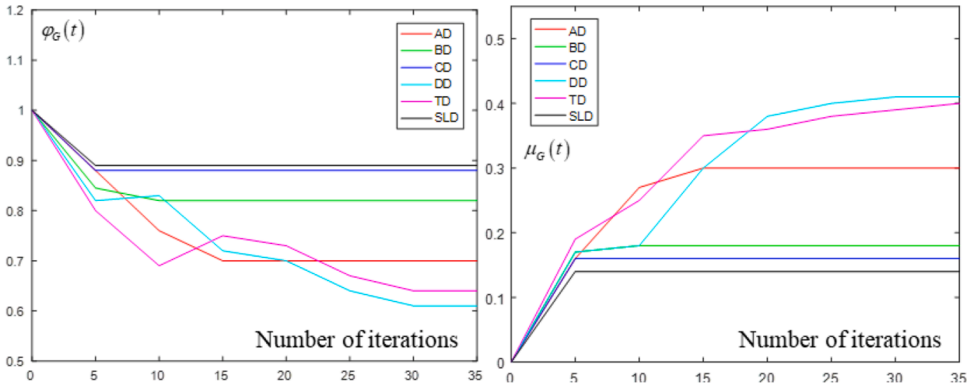


Fig. 4. The$\varphi_G(t)$and$\mu_G(t)$under different traffic load distribution strategies based on M-L model.

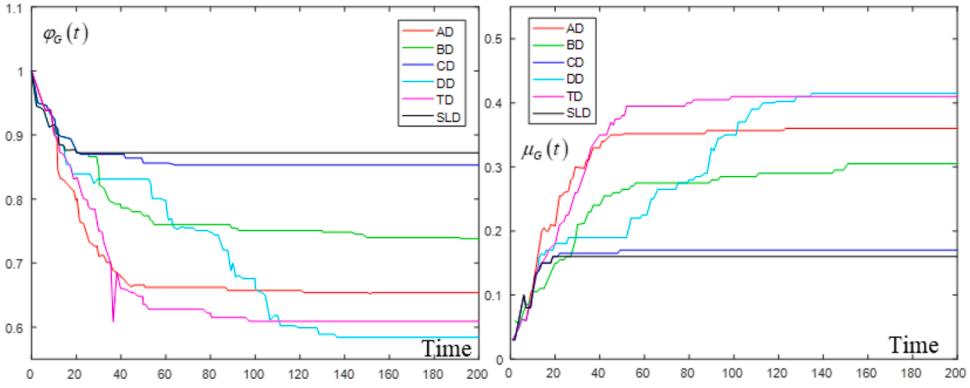


Fig. 5. The$\varphi_G(t)$and$\mu_G(t)$under different traffic load distribution strategies based on CA model.

the$\varphi_G(t)$decreases and tends to be stable with the increase of time, while the$\mu_G(t)$increases and tends to be stable with the increase of time. When the time is over 160, the vulnerability of RNDGT in Dalian remain unchanged. The node failure transmission trends of the two models are the same, which means the cascading failure model based on CA proposed in this paper is practicable and effective. (ii) For the two models under different traffic load distribution strategies, the vulnerability and the transmission time of RNDGT in Dalian have big differences among each other and have different fluctuations. That's because the recovery rate$\delta_i(t)$is considered into the models, the different traffic load distribution strategies take into account the geographical location and importance of the failed nodes and their neighbors in the network, which directly affects the relative load redistribution and the transmission time. (iii) For the M-L model, the number of failure iterations is used to describe the time characteristics of cascading failures in simulation, in actual practice, the number of failure iterations is not able to used to accurately reflect the specific cascading failure time point, hence, the results are unable to provide timely emergency rescue decisions for managers. (iv) For the value of vulnerability, compare with the M-L model, the CA based model under different traffic load distribution strategies have smaller value of vulnerability. That's because the CA based model considers the dynamic characteristics of load among the nodes, and M-L model ignores some important factors such as the distance among the nodes. Hence, the CA model has better feasibility and applicability.

(ii) The impacts of different settings of failure coefficient$\theta_i(t)$and recovery rate$\delta_i(t)$on the vulnerability

For the CA cascading failure model, we select nodes with number 28, 32, 76, 84 and 54 as the initial failed nodes (see Fig. 3). For all nodes, the adjustable parameter of load$\alpha = 1$, the tolerance coefficient of node$\beta_i = 0.1$, the recovery rate$\delta_i(t) = 0.1$, the distribution coefficient$\varpi = 1$. the failure coefficient$\theta_i(t)$is set increasing from 1.1 to greater than or equal to 1.9 with step 0.2. The traffic load distribution strategy is AD. The$\varphi_G(t)$and$\mu_G(t)$under different$\theta_i(t)$settings based on CA model is presented in Fig. 6. For the CA cascading failure model, we select nodes with number 28, 32, 76, 84 and 54 as the initial failed nodes. For all nodes, the adjustable parameter of load$\alpha = 1$, the tolerance coefficient of node$\beta_i = 0.1$, the failure coefficient$\theta_i(t) = 1.1$, the distribution coefficient$\varpi = 1$, the recovery rate$\delta_i(t)$is set increasing from 0.1 to 0.9 with step 0.2. The traffic load distribution strategy is AD. The$\varphi_G(t)$and$\mu_G(t)$under different$\delta_i(t)$settings based on CA model is presented in Fig. 7.

From Fig. 6, we can find that: (i) With the increase of$\theta_i(t)$, the$\varphi_G(t)$increases and tends to be stable while the$\mu_G(t)$decreases and tends to be stable. Higher$\theta_i(t)$means stronger ability of the node to handle the redundant load, thus enhancing the connectivity of the network and reducing the node failure rate. (ii) The$\theta_i(t)$reduces the vulnerability of the network to a certain extent, when it exceeds a certain threshold, the cascading failure degree of nodes can be minimized, in particular, when$\theta_i(t) \geq 1.9$, increasing$\theta_i(t)$can no longer reduce the network vulnerability.

According to Fig. 7, we can obtain: With the increase of$\delta_i(t)$, the$\varphi_G(t)$increases and tends to be stable while the$\mu_G(t)$decreases and tends to be stable. Higher$\delta_i(t)$means higher possibility of the node changes from the complete failure state into partial failure state. That is, the better the state of the complete failure node is, the stronger the load evacuation ability is, which enhances the connectivity of the network and reduces the node failure rate.

In order to reduce the network vulnerability and improve its stability and reliability, it is necessary to identify the key nodes in the network, and strengthen the construction and protection. Hence, based on the RNDGT in Dalian, we use point by point attack strategy on 154 nodes in the network to identify the key nodes. For all nodes, the adjustable parameter of load$\alpha = 1$, the tolerance coefficient of node$\beta_i = 0.1$, the failure coefficient$\theta_i(t) = 1.1$, the recovery rate$\delta_i(t) = 0.1$, the distribution coefficient$\varpi = 1$, the traffic load distribution strategy is AD. The$\varphi_G(t)$and$\mu_G(t)$with single failed node based on CA model is presented in Fig. 8. In addition, we select 10 key nodes in the network and present the related parameters, shown in Table 1.

According to the results presented in Fig. 8 and Table 1, we can obtain the following results: (i) The node 28, 32, 76, 84, 54, 94, 87, 89, 82 and 88 are the most important nodes of the RNDGT in Dalian. (ii) The nodes with higher node degree, betweenness and compactness do not necessarily have a greater impact on network vulnerability. For example, node 54, its node degree is 4, betweenness is 0.2082 and tightness is 0.0011, when cascading failure occurs in the node, the maximum connectivity is 0.6466, and the node failure rate is 0.3483. However, the node 28 has smaller node degree, betweenness and compactness, it has greater impact on network vulnerability when it fails.

As the conclusions, we find that: (i) When other parameters remain unchanged, the vulnerability of RNDGT decreases with the increase of failure coefficient$\theta_i(t)$. When the failure coefficient$\theta_i(t)$exceeds a certain threshold, increasing the failure coefficient will no longer reduce the network vulnerability. Therefore, when planning and designing the RNDGT, the failure coefficient$\theta_i(t)$can be appropriately increased to reduce the cascading failure damage. (ii) When other parameters remain unchanged, the vulnerability of RNDGT decreases with the increase of recovery rate$\delta_i(t)$. Hence, for the network management and protection, we can increase the node recovery rate$\delta_i(t)$by increasing the node protection resources and node rescue rate to avoid cascading failure spreading on the RNDGT. (iii) The nodes with higher node degree, betweenness and compactness do not necessarily have a greater impact on network vulnerability. Hence, for the management and protection of RNDGT, we should carry out the hierarchical management according to the impact of key nodes on network vulnerability, and focus on the

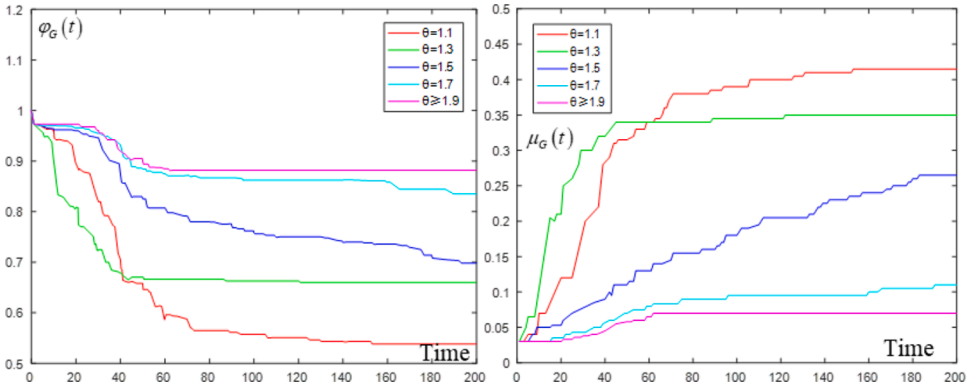


Fig. 6. The$\varphi_G(t)$and$\mu_G(t)$under different$\theta_i(t)$settings based on CA model.

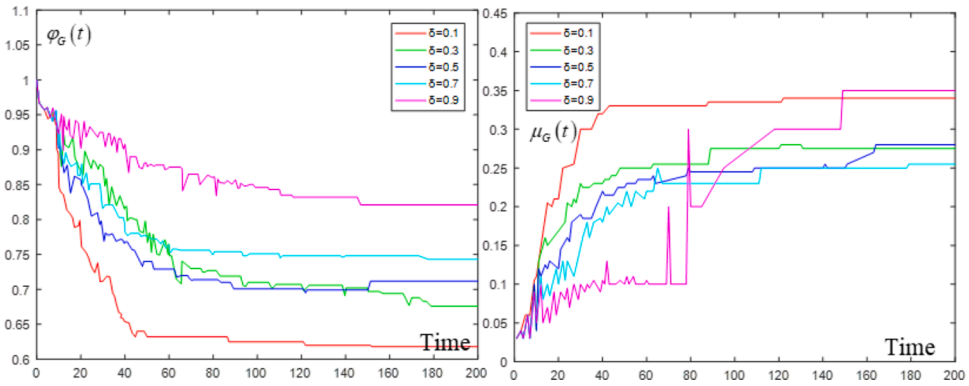


Fig. 7. The$\varphi_G(t)$and$\mu_G(t)$under different$\delta_i(t)$settings based on CA model.

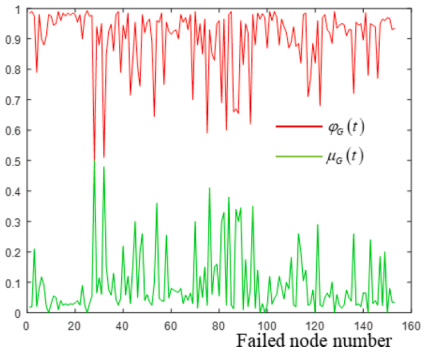


Fig. 8. The$\varphi_G(t)$and$\mu_G(t)$with single failed node based on CA model.

protection of nodes with high vulnerability. In addition, for the nodes with high vulnerability, we can reduce their vulnerability by appropriately increasing their capacity when planning and designing the nodes.

(iii) The impacts of different attack strategies on the vulnerability

In order to study the vulnerability of RNDGT in Dalian under different attack strategies, based on the CA model, the network nodes are attacked in descending order based on DA, BA and TA strategies. For all nodes, the adjustable parameter of load$\alpha = 1$, the tolerance coefficient of node$\beta_i = 0.1$, the failure coefficient$\theta_i(t) = 1.1$, the recovery rate$\delta_i(t) = 0.1$, the distribution coefficient$\varpi = 1$, the different traffic load distribution strategies are compared and discussed. Assume that the network is in a serious failure state when$\varphi_G(t) \leq 0.4$, or$\mu_G(t) \geq 0.6$. Firstly, we calculate the degree, betweenness and tightness of each node of RNDGT in Dalian, and rank nodes in descending order according to the calculation results. For each kind of attack strategy, we choose top 20 nodes as the attacked nodes: For DA strategy, the initial failed nodes are 116, 48, 143, 141, 136, 133, 126, 125, 121, 115, 110, 108, 101, 100, 96, 92, 91, 89, 86 and 81 (in descending order, see Fig. 9). For BA, the initial failed nodes are 92, 80, 54, 48, 51, 86, 98, 102, 45, 57, 52, 34, 133, 116, 67, 100, 91, 117, 29 and 66 (in descending order, see Fig. 9). For TA, the initial failed nodes are 54, 57, 48, 66, 67, 45, 80, 79, 53, 51, 92, 49, 91, 56, 62, 87, 47, 52, 42 and 78 (in descending order, see Fig. 9).

The results of vulnerability are presented in Fig. 10, Fig. 11 and Fig. 12, respectively. The horizontal ordinate of Figs. 10–12 shows the number of attacked nodes, the increase in the number of nodes follows the series of the numbers list before (in descending order, see Fig. 9). Under such attack combinations, we think the$\varphi_G(t)$under different traffic assignment strategies will decrease (with deceleration) and tend to be stable gradually, and the$\mu_G(t)$will increase (with deceleration) and tend to be stable generally.

After analyzing Fig. 10, we can obtain: (i) Under DA attack strategy, with the increase of the attacked nodes, the$\varphi_G(t)$under different traffic assignment strategies decrease and tend to be stable gradually, and the$\mu_G(t)$increase and tend to be stable generally. (ii) When the number of attacked nodes is 2, the decline rate of the$\varphi_G(t)$and the rising rate of$\mu_G(t)$are particularly obvious. The vulnerability of RNDGT in Dalian is lower under the multi-nodes cascading failures. (iii) The impacts of the 6 traffic load distribution strategies on network vulnerability are quite different, SLD strategy is the best, followed by AD, DD strategy is the worst. In the process of evacuating the load of failed nodes, SLD fully considers the redundant bearing capacity of neighbor nodes. The smaller the redundant load is, the higher the failure risk of neighbor node is, the less evacuation traffic load it receives, which can significantly control the impact of cascading failures on the neighbor nodes and reduce the vulnerability of the network. (iv) For all the 6 traffic load distribution strategies, when the number of attacked nodes is over 6,$\varphi_G(t) \leq 0.4$, or$\mu_G(t) \geq 0.6$, the network is in a serious failure state.

After analyzing Fig. 11, we can obtain: (i) Under BA attack strategy, with the increase of the attacked nodes, the$\varphi_G(t)$under different traffic assignment strategies decrease and tend to be stable gradually, and the$\mu_G(t)$increase and tend to be stable generally. (ii) When the number of attacked nodes is 2, the decline rate of the$\varphi_G(t)$and the rising rate of$\mu_G(t)$are particularly obvious. The vulnerability of RNDGT in Dalian is lower under the multi-nodes cascading failures. (iii) From the perspective of$\varphi_G(t)$, when the number of attacked nodes is greater than 8, BD strategy is the best, and the$\varphi_G(t)$under other traffic load distribution strategies are less than 0.4. The network is in a serious failure state and has high vulnerability. When the number of attacked nodes is less than 8, the SLD strategy is optimal, which can significantly control the impact of cascading failures on network and reduce the vulnerability of the network. (iv) From the perspective of$\mu_G(t)$, when the number of failed nodes is small, the SLD strategy is better, followed by BD strategy. (v)

Table 1
Parameter values of 10 key nodes under single node failure.

Node	$\varphi_G(t)$	$\mu_G(t)$	$d_i(t)$	$B_i(t)$	$TD_i(t)$	Node	$\varphi_G(t)$	$\mu_G(t)$	$d_i(t)$	$B_i(t)$	$TD_i(t)$
28	0.4864	0.5002	3	0.0099	0.0008	**94**	0.6311	0.3398	3	0.0222	0.0009
32	0.5168	0.4904	3	0.0453	0.0008	**87**	0.6618	0.3341	3	0.0315	0.0010
76	0.5962	0.4022	3	0.0562	0.0009	**89**	0.6734	0.3291	4	0.0836	0.0008
84	0.6061	0.3724	3	0.0039	0.0009	**82**	0.6936	0.3269	3	0.0691	0.0009
54	0.6466	0.3483	4	0.2082	0.0011	**88**	0.6685	0.3079	3	0.0254	0.0009

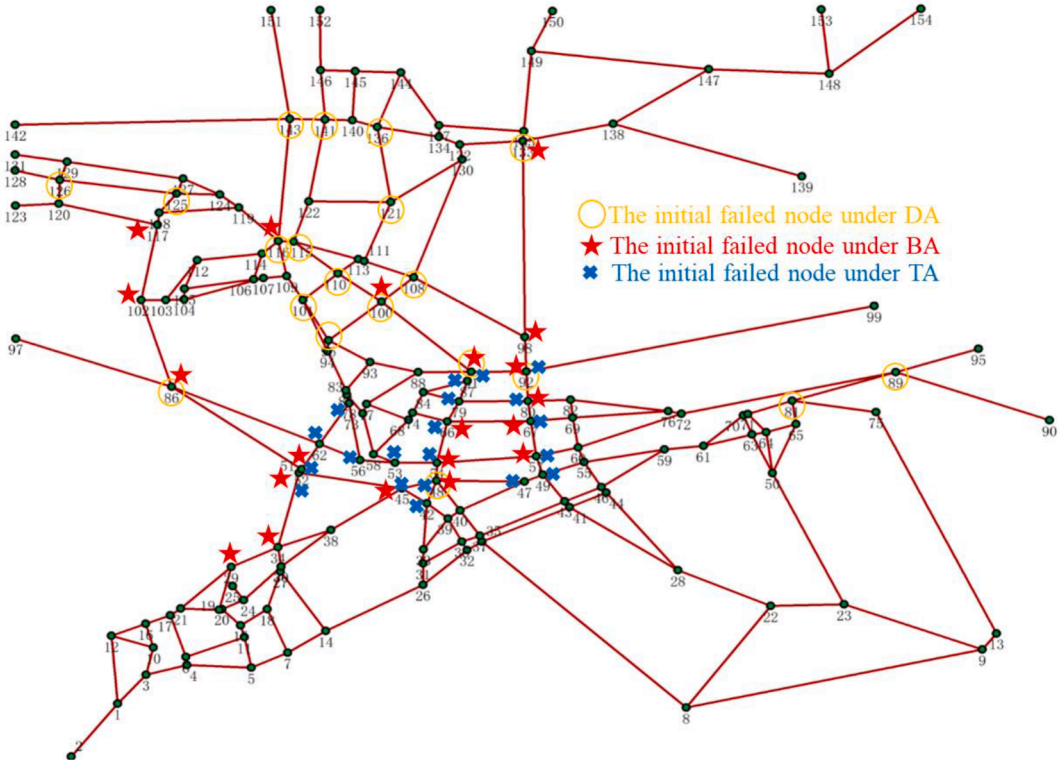


Fig. 9. The distribution of failed nodes under DA, BA and TA.

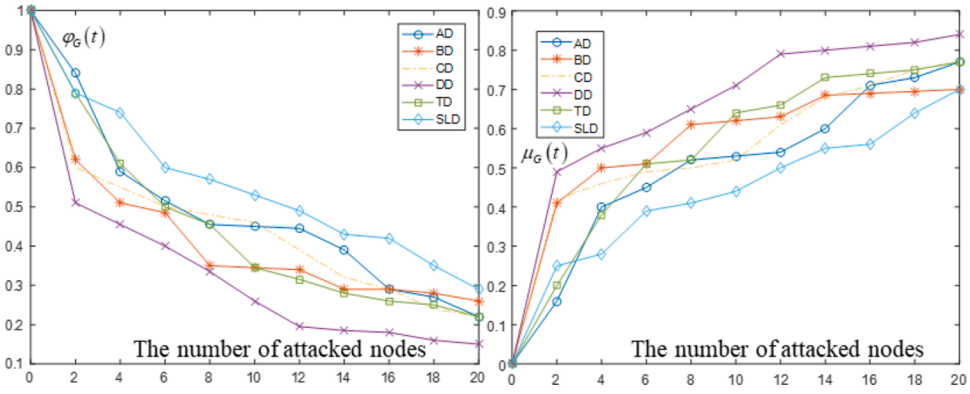


Fig. 10. The$\varphi_G(t)$and$\mu_G(t)$under different traffic load distribution strategies based on DA.

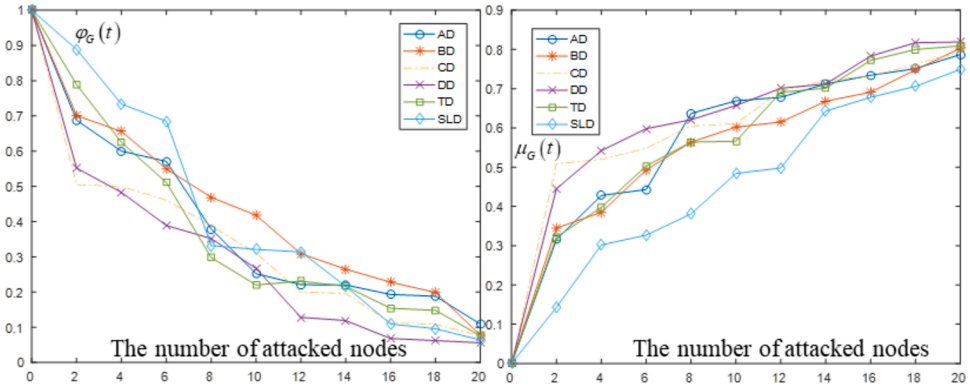


Fig. 11. The$\varphi_G(t)$and$\mu_G(t)$under different traffic load distribution strategies based on BA.

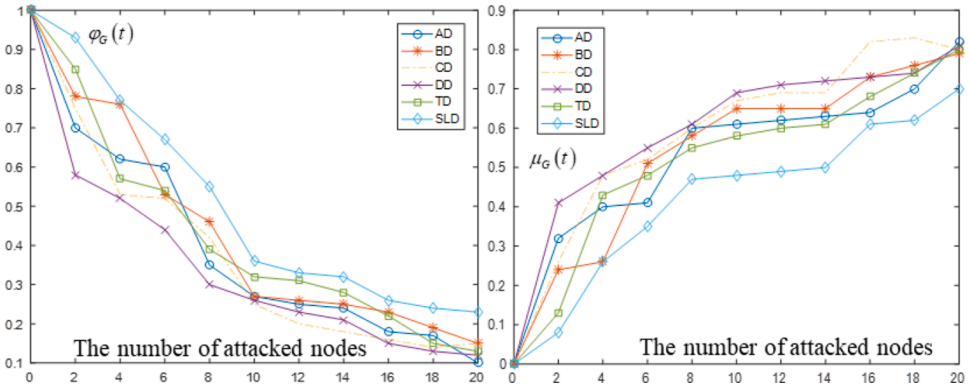


Fig. 12. The$\varphi_G(t)$and$\mu_G(t)$under different traffic load distribution strategies based on TA.

For all the 6 traffic load distribution strategies, DD strategy is the worst. When the number of attacked nodes is over 6,$\varphi_G(t) \leq 0.4$, or$\mu_G(t) \geq 0.6$, the network is in a serious failure state.

After analyzing Fig. 12, we can obtain: (i) Under TA attack strategy, with the increase of the attacked nodes, the$\varphi_G(t)$under different traffic assignment strategies decrease and tend to be stable gradually, and the$\mu_G(t)$increase and tend to be stable generally. (ii) When the number of attacked nodes is 2, the decline rate of the$\varphi_G(t)$and the rising rate of$\mu_G(t)$are particularly obvious. The vulnerability of RNDGT in Dalian is lower under the multi-nodes cascading failures. (iii) The impacts of the 6 traffic load distribution strategies on network vulnerability are quite different, SLD strategy is the best, which can significantly control the impact of cascading failures on the neighbor nodes and reduce the vulnerability of the network. (iv) For all the 6 traffic load distribution strategies, DD strategy is the worst. When the number of attacked nodes is over 8,$\varphi_G(t) \leq 0.4$, or$\mu_G(t) \geq 0.6$, the network is in a serious failure state.

As the conclusions, we find that: (i) From the attack strategy perspective, TA strategy has the least damage to network vulnerability, and DA strategy has the greatest damage to network vulnerability. Therefore, we should pay more attention to the network vulnerability under DA strategy, for safety management and emergency rescue, we can increase network protection resources to reduce cascading failure damage. (ii) From the traffic load distribution strategy perspective, when the intentional attack occurred, SLD strategy should be firstly selected under the descending attack strategy of DA, BA and TA. Among the 6 traffic load distribution strategies, DD strategy is the worst, especially when the number of attacked nodes is more than 6.

7. Conclusion and further study work

In this paper, we analyze the vulnerability of road network for dangerous goods transportation (RNDGT) under cascading failure considering intentional attack. Most of previous cascading failure works assume that there are three kinds of node states in the network including normal state, pending state and failure state. The nodes in the failure state are completely blocked without recovery ability in the simulation time. We introduce the time characteristics of load distribution and node recovery ability into the previous cascading failure models, subdivide the state of failed node into normal state, partial failure state and complete failure state. Most previous researches only discuss the network performance under the average load distribution of traffic volume. In this paper, we choose Average Distribution (AD), Betweenness Distribution (BD), Capacity Distribution (CD), Degree Distribution (DD), Tightness Distribution (TD) and Surplus Load Distribution (SLD) to study the load re-distribution of failed nodes. In addition, we select and compare the node attack strategies include Degree Attack (DA), Betweenness Attack (BA) and Tightness Attack (TA), the nodes with higher node degree, betweenness or compactness are selected to attack each time. By referring the application of cellular automata applied in epidemic spreading field, we establish a new cascading failure model of RNDGT, and explore the vulnerability of RNDGT under different intentional node attack strategies and different traffic load distribution strategies, the two parameters including improved maximum connectivity and node failure rate based on node degree are applied to analyze the vulnerability of RNDGT.

A case study is conducted by using the RNDGT and the transportation volume of Dalian, China as the background. The previous M-L model is applied as the comparison approach. M-L model uses the number of iterations to represent the time characteristics of network vulnerability, the CA cascaded failure model can not only measure the degree of network vulnerability, but also describe the time change trend of vulnerability. When other parameters remain unchanged, vulnerability increases with the increase of failure coefficient, and decreases with the increase of node recovery rate. In particular, when the failure coefficient exceeds a certain threshold, the increase of failure coefficient will no longer reduce the network vulnerability. The model can identify the key nodes of RNDGT in Dalian, therefore, in the process of network defense resource allocation and security management, we should focus on protecting the nodes with high vulnerability. TA strategy has the least impact on increasing network vulnerability, SLD strategy is the best to reduce network vulnerability.

The works in the future include: (i) We set that the node in complete failure state can be transformed into partial failure state after recovery, we can discuss whether such node can be transformed into normal node directly. (ii) In actual practice, when the nodes of the RNDGT fail, the traffic load distribution speed in different intersections and edges is not the same, in this paper we ignore the difference of load distribution speed. (iii) We ignore the impact of different types of dangerous goods on network vulnerability, we can consider the types of dangerous goods into the vulnerability of RNDGT under cascading failure. (iv) There are differences between epidemic spreading based cascading failure model and cascading failure model of RNDGT, e.g., in the epidemic spreading based cascading failure model, the virus can self-replicate and has a certain latency, and its individual state change is more complex; (v) In this paper, we assume that the demand of dangerous goods by road and the traffic flows will remain unchanged in a short time after the attack occurred. However, as a result of a major anthropogenic or natural event occurring on the transport network, the dangerous goods transport demand may be reduced or be postponed, the transportation demand of dangerous goods might be elastic and the traffic flows are also reduced during the disruption of a link of the network. Such situations can be considered into the future study; (vi) In addition, the attacks might have impact on the dangerous goods themselves, the derivative accidents such as explosion and combustion of dangerous goods caused by the intentional attack might happen, and other neighboring nodes/edges might be affected by the damaged goods, such situations can also be considered in the future work.

Author statement

The authors claim that none of the material in the paper has been published or is under consideration for publication elsewhere. [65]

Declaration of Competing Interest

The authors declared that we have no conflicts of interest to this work.

Acknowledgments

This research was jointly supported by the National Natural Science Foundation of China (71173177), Youth Fund of National Natural Science Foundation of China (72001179) and International Science and Technology Innovation Cooperation Project of Science & Technology Department of Sichuan Province (2021YFH0106) and Basic Research Fund of Central University (2682021CX052).

References

[1] Adnan M, Tariq M. Cascading overload failure analysis in renewable integrated power grids. Reliab Eng Syst Saf 2020;198:106887.
[2] Alexander ED, Blazhe G, Giovanni S. Quantitative comparison of cascading failure models for risk-based decision making in power systems. Reliab Eng Syst Saf 2020; 198:106877.
[3] Amoroso S, Patt Y. Decision procedures for surjectivity and injectivity of parallel maps for tessellation structures. Comput Syst Sci 1972;6:448–64.
[4] Andersson SE. Safe transport of dangerous goods: road, rail or sea? A screening of technical and administrative factors. Eur J Operat Res 1994;75(3):499–507.
[5] Augusto VD, Héctor RD, Pere SS. Vulnerability of the European air transport network to major airport closures from the perspective of passenger delays: Ranking the most critical airports. Transp Res Part A 2017;96:119–45.
[6] Azzolin A, Leonardo DO, Francesco C, Enrico Z. Electrical and topological drivers of the cascading failure dynamics in power transmission networks. Reliab Eng Syst Saf 2018;175:196–206.
[7] Bęczkowska S. The method of optimal route selection in road transport of dangerous goods. Transp Res Proced 2019;40:1252–9.
[8] Benekos I, Diamantidis D. On risk assessment and risk acceptance of dangerous goods transportation through road tunnels in Greece. Saf Sci 2017;91:1–10.
[9] Berdica K. An introduction to road vulnerability: what has been done, is done and should be done. Transp Policy 2002;9(2):117–27.
[10] Chiou SW. A resilience-based signal control for a time-dependent road network with hazmat transportation. Reliab Eng Syst Saf 2020;193:106570.
[11] Chong PY, Shuai B. Cascading failure model and coupling properties for interdependent networks of hazardous materials transportation. J Transp Syst Eng Inf Technol 2015;15(5):150–6.
[12] Conca A, Ridella C, Sapori E. A risk assessment for road transportation of dangerous goods: a routing solution. Transp Res Proc 2016;14:2890–9.
[13] Daganzo CF. In traffic flow, cellular automata=kinematic waves. Transp Res Part B 2006;40:396–403.
[14] D'Este GM, Taylor MAP. Network vulnerability: an approach to reliability analysis at the level of national strategic transport networks. In: Proceeding of the 1st International Symposium on Transportation Network Reliability (INSTR); 2003. 2003.
[15] Dong JS, Wu YW, Lu QC. Vulnerability analysis of urban road network topology under rainfall. J Transp Syst Eng Inf Technol 2015;15(5):109–22.
[16] Dong JS, Jing WG, Lu QC. Vulnerability evaluation of road network considering congestion propagation effect. J Chongq Univ Technol (Natural Sci) 2015;29(8): 55–60.
[17] Dui HY, Meng XY, Xiao H, Guo JJ. Analysis of the cascading failure for scale-free networks based on a multi-strategy evolutionary game. Reliab Eng Syst Saf 2020; 199:106919.
[18] Erath A, Birdsall J, Axhausen KW, Hajdin R. Vulnerability assessment of the Swiss road network. In: Proceedings of the 88th Transportation Research Board Annual Meeting; 2009. p. 1–17. 2009.
[19] Faghih-Roohi S, Ong YS, Asian S, Zhang AN. Dynamic conditional value-at-risk model for routing and scheduling of hazardous material transportation networks. Ann Operat Res 2016;247(2):715–34.
[20] Fresnadillo, M.J., García, E., García, J.E., Rey, A.M.D., Sánchez, G.R., 2009. A SIS epidemiological model based on cellular automata on graphs. Proceedings of the nternational Work-conference on Artificial Neural Networks. Springer-Verlag, 1055–1062.
[21] Fresnadillo MJ, García E, García JE, Rey AMD, Sánchez GR. A model based on cellular automata to simulate a sis epidemic disease. J Pure Appl Math Adv Appl 2011;5(2):125–39.
[22] Fu XW, Yang YS. Modeling and analysis of cascading node-link failures in multi-sink wireless sensor networks. Reliab Eng Syst Saf 2020;197:106815.
[23] Ge HX, Zhu HB, Dai SQ. Cellular automata traffic flow model considering intelligent transportation system. Acta Phys Sinica 2005;54(10):4621–6.
[24] Goodrum CJ, Shields CPF, Singer DJ. Understanding cascading failures through a vulnerability analysis of interdependent ship-centric distributed systems using networks. Ocean Eng 2018;150:36–47.
[25] Guidotti R, Gardoni P, Chen Y. Network reliability analysis with link and nodal weights and auxiliary nodes. Struct Saf 2017;65:12–26.
[26] Hu P, Fan WL. Mitigation strategy against cascading failures considering vulnerable transmission line in power grid. Phys A 2020;540:123230.
[27] Hua W, Yue YX, Wei ZL, Chen JH, Wang WR. A cellular automata traffic flow model with spatial variation in the cell width. Phys A 2020;556:124777.
[28] Huang WC, Shuai B, Pang L, Yang ZQ. Research on coupling coordination degree based method for assessing risk in road dangerous goods transport system. China Safety Sci J 2016;26(6):117–22.
[29] Husdal J. The vulnerability of road networks in a cost-benefit perspective. In: Proceedings of the 84th Transportation Research Board Annual Meeting; 2005. p. 9–13. 2005.
[30] Jenelius E, Petersen T, Mattsson LG. Importance and exposure in road network vulnerability analysis. Transp Res Part A Pol Pract 2006;40(7):537–60.
[31] Jenelius E, Mattsson L. Road network vulnerability analysis: Conceptualization, implementation and application. Comput Environ Urban Syst 2015;49:136–47.
[32] Kerner BS, Klenov SL, Wolf DE. Cellular automata approach to three-phase traffic theory. J Phys A Gen Phys 2002;35(47):9971–10013.
[33] Lee L, Hu P. Vulnerability analysis of cascading dynamics in smart grids under load redistribution attacks. Electrical Power Energy Syst 2019;111:182–90.
[34] Lei L, Ba KW. Traffic vulnerability assessment method based on cascading failure model. J Highway Transp Res Develop 2013;9:302–5.
[35] Liu QX, Jin Z. Cellular automata modelling of SEIRS. Chin Phys 2015;14(7): 1370–7.
[36] Lundin J, Antonsson L. Road tunnel restrictions-Guidance and methods for categorizing road tunnels according to dangerous goods regulations (ADR). Saf Sci 2019;116:170–82.
[37] Mattsson LG, Jenelius E. Vulnerability and resilience of transport systems-A discussion of recent research. Transp Res Part A 2015;81:16–34.
[38] Meng Q, Weng JX. An improved cellular automata model for heterogeneous work zone traffic. Transp Res Part C 2011;19:1263–75.
[39] Moreno Y, Gómez JB, Pacheco AF. Instability of scale-free networks under node-breaking avalanches. Europhys Lett 2002;58(4):630–6.
[40] Motter AE, Lai YC. Cascade-based attacks on complex networks. Phys Rev E 2002; 66(6):065102.
[41] Nagel K, Schreckenberg M. A cellular automata model for freeway traffic. J De Physique I., 1992;2(12):2221–9.
[42] Niu SF, Ukkusuri SV. Risk Assessment of Commercial dangerous-goods truck drivers using geo-location data: a case study in China. Accident Anal Prevent 2020; 137:105427.
[43] Purdy G. Risk analysis of the transportation of dangerous goods by road and rail. J Hazard Mater 1993;33(2):229–59.
[44] Ruan X, Zhou JY, Tu HZ, Jin ZR, Shi XF. An improved cellular automaton with axis information for microscopic traffic simulation. Transp Res Part C 2017;78:63–77.
[45] Scott DM, Novak DC, Aultman-Hall L, Guo F. Network robustness index: a new method for identifying critical links and evaluating the performance of transportation networks. J Transp Geogr 2016;14(3):215–27.
[46] Shuang Q, Zhang MY, Yuan YB. Node vulnerability of water distribution networks under cascading failures. Reliab Eng Syst Saf 2014;124:132–41.
[47] Song YR, Jiang GP, Xu JG. An epidemic spreading model in adaptive networks based on cellular automata. Acta Phys Sinica 2011;60(12). 120509-1-120509-10.
[48] Sun LS, Huang YC, Chen YY, Yao LY. Vulnerability assessment of urban rail transit based on multi-static weighted method in Beijing, China. Transp Res Part A Pol Pract 2018;108:12–24.
[49] Takayasu M, Takayasu H. 1/F noise in a traffic model, 1. World Scientific Publishing Company; 1993. p. 860–6.
[50] Tian JF, Li GY, Treiber M, Jiang R, Jia N, Ma SF. Cellular automaton model simulating spatiotemporal patterns, phase transitions and concave growth pattern of oscillations in traffic flow. Transp Res Part B Methodol 2016;93:560–75.
[51] Timmerman P. Vulnerability resilience and collapse of society. Toronto: Institute for Environmental Studies; 1981. 1981.
[52] Wang YQ, Jiang GP. Epidemic spreading in complex networks with spreading delay based on cellular automata. Acta Phys Sinica 2011;60(8):110–8.
[53] White SH, Rey AMD, Sánchez GR. Modeling epidemics using cellular automata. Appl Math Comput 2011;186(1):193–202.
[54] Wolfram S. Statistical mechanics of cellular automata. Rev Mod Phys 1983;55(3): 601–44.
[55] Wolfram S. Theory and applications of cellular automata. Singapore World Scientific Publication; 1986. 1986.
[56] Xu Y, Dong LY, Dai SQ. An improved one-dimensional cellular automata model of traffic flow and the effect of deceleration probability. Acta Physica Sinica 2001;50 (3):445–9.
[57] Yang SH, Chen WR, Zhang XX, Yang WQ. A graph-based method for vulnerability analysis of renewable energy integrated power systems to cascading failures. Reliab Eng Syst Saf 2021;207:107354.
[58] Ye Q. Vulnerability analysis of rail transit network based on complex network theory. China Safety Sci J 2012;22(2):122–6.
[59] Zhang YL, Yang ND. Vulnerability analysis of interdependent R&D networks under risk cascading propagation. Phys A 2018;505:1056–68.
[60] Zhang C, Xu X, Dui HY. Analysis of network cascading failure based on the cluster aggregation in cyber-physical systems. Reliab Eng Syst Saf 2020;202:106963.

[61] Zhang L, Wen HY, Lu J, Li SB, Lei D. Vulnerability assessment and visualization of large-scale bus transit network under route service disruption. Transp Res Part D Transp Environ 2020;88:102570.
[62] Zhao HT, Zhao X, Lu JC, Xin LY. Cellular automata model for Urban Road traffic flow Considering Internet of Vehicles and emergency vehicles. J Comput Sci 2020; 47:101221.
[63] Zeng JW, Qian YS, Mi PF, Zhang CY, Yin F, Zhu LP, Xu DJ. Freeway traffic flow cellular automata model based on mean velocity feedback. Phys A 2021;562: 125387.
[64] Zheng Y. Vulnerability analysis of urban road traffic network considering congestion effect. Huazhong University of science and technology; 2015. 2015.
[65] Zhong H, Wang J, Yip TL, Gu Y. An innovative gravity-based approach to assess vulnerability of a Hazmat road transportation network: a case study of Guangzhou. China. Transp Res Part D Transp Environ 2018;62:659–71.
[66] Zhong JL, Sanhedrai H, Zhang FM, Yang Y, Guo S, Yang SK, Li DQ. Network endurance against cascading overload failure. Reliab Eng Syst Safety 2020;201: 106916.
[67] Zhou J, Coit DW, Felder FA, Wang DL. Resiliency-based restoration optimization for dependent network systems against cascading failures. Reliab Eng Syst Saf 2021;207:107383.