CHANG CHEN
JIKUN GUO
QIXIN ZHANG
SHIFU ZHANG
YI WANG
and
TENGFEI ZHANG

Structural invulnerability evaluation of complex multi-layer emergency logistics system based on interdependent network theory

Emergency logistic system is quite important for natural disaster recue and other unexpected incidents treatment. At present, most relative modelling and analyzing research on logistic network invulnerability is based on a single network, and does not take the interaction between networks into account. This paper proposes the complex multi-layer logistic model consists of command control network, space communication network and physical transportation network based on interdependent network theory. The result of network invulnerability research shows that the three-layer interdependent network model is more precisely and conform to the actual situation of emergency logistic system operation. Moreover, the invulnerability evaluation method proposed in this paper is more accurate and detailed than the traditional method. This conclusion can provide references for the designing of emergency logistics system with better invulnerability and applied to other areas research.

Keywords: *Invulnerability evaluation; multi-layer system; emergency logistics; interdependent network theory.*

1. Introduction

Emergency logistic system play an important role in the natural disaster rescue and emergency public events, etc. The damage results in earthquakes, floods, landslides, debris flow and other natural disaster reflect the vulnerability and instability characteristics of logistic network. Thus, it is very important and meaningful to design a logistic network with better reliability. In fact, it is very difficult to measure and control the degree of interference and damage that the natural disasters are occurred on logistic system. Many experts and scholars have carried out relevant research on this aspect. In 1998, Watts and Strogatz published an article entitled "Collective dynamics of small world networks" in *Nature* magazine, highlighting the small world characteristics of real world (Watts S. H. and Strogatz, 1998). In 1999, Barabasi and Albert wrote the "emergence of scaling in random networks" in *Science* journal, discovering the scale-free properties of network (Barabasi and Albert, 1999). These two innovative articles opened a new area for complex network research. After that, in 2002, Pettr Holme and Beom Kim published an article entitled "Attack vulnerability of complex network" in the *Physical Review E*, which systematically summarizes the response of complex network reliability in different attack modes, and proposed the idea of using the maximum connected subgraph and network efficiency to measure network performance (Holme, et al., 2002). Besides, in response to heavy demand for emergency logistics, Li, Xiaohui introduced an approach based on hierarchical network theory to solve the complexity of highway transportation network (Li and Tan, 2011). Chen, Chunxia analyzed the logistic network's invulnerability by the average inverse geodesic length and the size of the largest connected subgraph (Chen and Wang, 2012). Li Huang proposed the conception and evaluation indexes of emergency logistics network connecting reliability to construct evaluation index system of complex network reliability, and described these indexes quantitatively to evaluate the network connecting reliability (Huang, et al., 2013). Hong, Jae-Dong considered simultaneous strategic and operational planning for the emergency logistics network (ELN) design (Hong, et al., 2015).

Most scholars' research on logistic networks is based on a single network for modelling and analysis (Kuhnle, et al., 2017, (Wang, et al., 2016), and does not take the interaction between networks into account (Guo, et al., 2017). However, in the real world, each functional network is more or less connected with other networks, such as physical dependency, logical dependency, energy or information

Messrs. Chang Chen, Jikun Guo, Professor, Service Command Department, Qixin Zhang, Associate Professor, Oil Department, Shifu Zhang, Professor, National Engineering Research Center for Disaster & Emergency Relief Equipment, Yi Wang, Doctoral Student, Service Command Department and Tengfei Zhang, Doctoral Student, Oil Department, Army Logistics University of PLA, Chongqing 401 331, China. Corresponding author e-mail: 408430734@qq.com

exchanges, etc. Strictly speaking, entirely isolated network does not exist in reality. Once a network node fails, the impact of the failure will be spread and amplified due to the inter-network connection. Eventually, a small failure may have catastrophic consequences for the entire system.

Different from previous studies, this paper proposes the complex multi-layer model for emergency logistics system based on interdependent network theory. During the structural invulnerability evaluation, the inter-relationships between networks have been taken into consideration appropriately, which is more in accordance with the actual situation of the system.

2. Multi-layer emergency logistics system model

Emergency logistics network is a complex network system. In the operation process, all levels of members, such as the command agencies, security bases, material supply stations, reserve warehouses, demand units, and various entities, such as airports, stations, ports are interrelated to form an organic whole based on the command relationship, communication lines and transportation lines. According to the command flow, information flow and material flow in the emergency logistics network, the emergency logistics network has been modelled as a multi-layer system composed of command and control network, space communication network and physical transportation network.

2.1 Command and control network model

The command and control network can be described as $T = (V_T, E_T)$, as shown in Fig.1, where $V_T = \{t_1, t_2, t_{3,...,} t_{NT}\}$ is the set of nodes, indicating the main control part and the object. $N_T = |V_T|$ represents the number of command nodes, E_T is the set of edges, indicating the relationships between the command parts and control objects. Command and control relations mainly include subordination, coordination and service guidance. For the same level of command and control nodes, if there is a synergy or cooperative relationship between the two nodes, then the two nodes in same level will be connected. If there are subordinate or service guidance relationships between the two nodes in different level, there will be a connection edge between the two nodes.

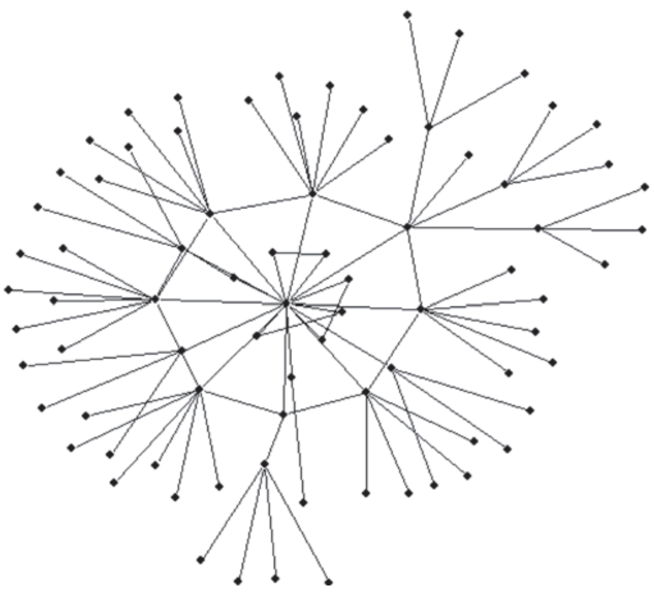


Fig.1 The schematic diagram of command and control network model

2.2 Space communication network model

The space communication network can be described as $L = (V_L, E_L)$, as shown in Fig 2, where $V_L = \{t_1, t_2, t_{3,...,} t_{NL}\}$ is the set of nodes, denoting the communication station, communication hub and communication terminal in each communication network. $N_L = |V_L|$ represents the number of communication nodes, E_L is the set of edges, indicating the physical circuit that transmits information between communication nodes. The physical connections between communication nodes may include wireless, wired, and many other ways.

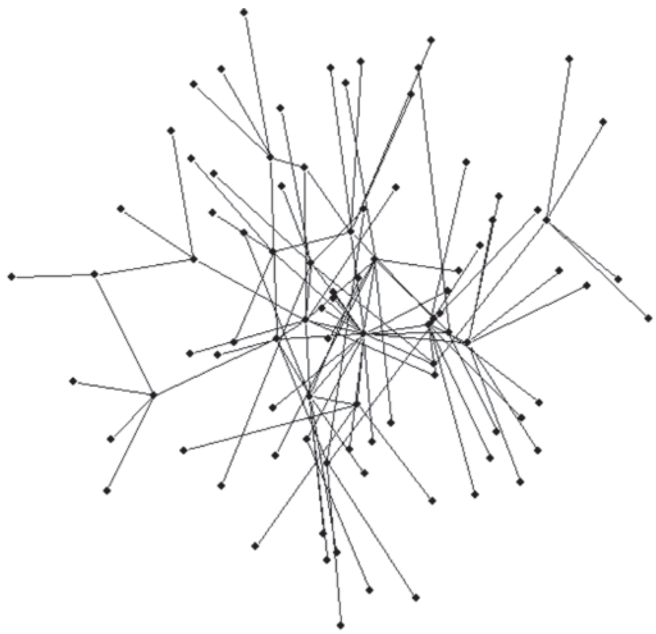


Fig.2 The schematic diagram of space communication network model

2.3 Physical transportation network model

Physical transportation network can be described as $C = (V_C, E_C)$, as show in Fig 3, where $V_C = \{t_1, t_2, t_{3,...,} t_{NC}\}$ is the set of nodes, indicating the airport, station, port, terminal and other physical nodes. $N_c = |V_c|$ represents the number of physical transportation nodes, is the set of edges, indicating the routes between the entity nodes including the railway line, highway line, and the waterway line.

2.4 Interdependent network model

D represents the multi-layer dependency model, as shown in Fig 4, which consists of D_1 the relationship between the command-control network *T* and the space communication network *L*, and D_2 the relationship between the space

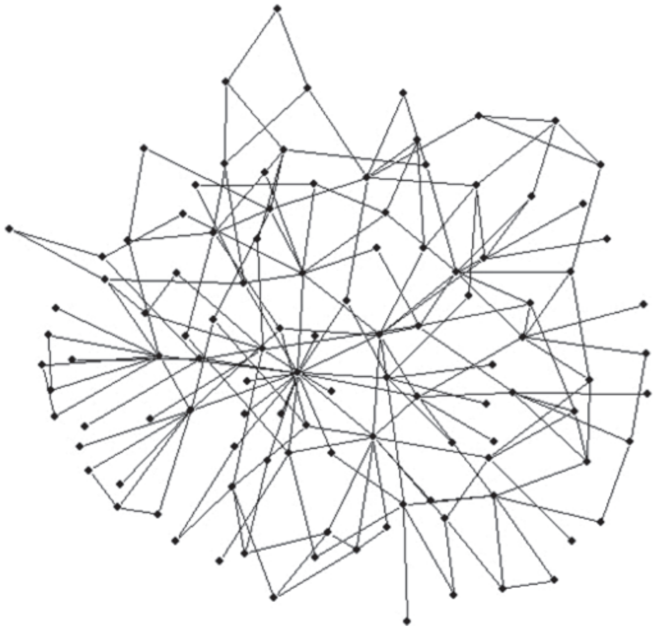


Fig.3 The schematic diagram of physical transportation network model

communication network L and physical transportation network C.

$$D = D_1 \cup D_2 \quad \dots \quad (1)$$

$$D_1 = E_{D1} = \left\{(t_1,l_1),(t_2,l_2),\dots,(t_i,l_j)\right\} \quad \dots \quad (2)$$

$$D_2 = E_{D2} = \left\{(l_1,c_1),(l_2,c_2),\dots,(l_i,c_j)\right\} \quad \dots \quad (3)$$

Equation (1)-(3) denoting the note set which relies on others. M_D represents the construction matrix of multi-layer dependency model D. In M_{D1}, elements in command-control network T has been filled the rows of matrix and elements in space communication network L has been filled with the columns of matrix. In equation (4), $m_{D1_{ij}}=1$ illustrating a dependency relationship between the command-control network note v_i and space communication network note l_j. $m_{D1_{ij}}=0$ stating the dependency relationship does not exist.

$$m_{D1_{ij}} = \begin{cases} 1 & (t_i,l_j) \in E_D \\ 0 & (t_i,l_j) \notin E_D \end{cases} \quad \dots \quad (4)$$

In M_{D2}, elements in space communication network L has been filled the rows of matrix and elements in physical transportation network C has been filled with the columns of matrix. In equation (5), $m_{D2_{ij}}=1$ illustrating a dependency relationship between space communication network note l_i and physical transportation network note c_j. $m_{D2_{ij}}=0$ stating the dependency relationship does not exist.

$$m_{D2_{ij}} = \begin{cases} 1 & (\mathrm{l}_i,\mathrm{c}_j) \in E_D \\ 0 & (\mathrm{l}_i,\mathrm{c}_j) \notin E_D \end{cases} \quad \dots \quad (5)$$

The interdependent network model can be set up based on three basic models proposed before. $G = <V,E>$ denoting the multi-layer dependency network, as shown in Fig.4, and it can be expressed as follow:

$$\begin{cases} G = <T,L,C,D> = <V,E> \\ T = (V_T,E_T) \\ V_T = \left\{t_1,t_2,\dots,t_i,\dots,t_{N_T}\right\} \quad i \le N_T \\ L = (V_L,E_L) \\ V_L = \left\{l_1,l_2,\dots,l_j,\dots,l_{N_L}\right\} \quad j \le N_L \\ C = (V_C,E_C) \\ V_C = \left\{c_1,c_2,\dots,c_k,\dots,c_{N_C}\right\} \quad k \le N_C \\ D = D_1 \cup D_2 = \left\{(t_1,l_1),(t_2,l_2),\dots,(t_i,l_j)\right\} \\ \qquad \cup \left\{(l_1,c_1),(l_2,c_2),\dots,(l_i,c_j)\right\} \\ V = V_T \cup V_L \cup V_C \\ E = E_T \cup E_L \cup E_C \cup E_{D1} \cup E_{D2} \\ N = N_T + N_L + N_C \quad N_T \le N_L \le N_C \end{cases} \quad \dots \quad (6)$$

In equation (6), G denotes the topology of the emergency logistics network. V denotes the set of emergency logistics network components (command organization, communication node, transportation hub), consisting of V_T, V_L and V_C. E denotes the connection relation of nodes in the emergency logistics network, consisting of E_T, E_L, E_C, E_{D1} and E_{D2}. N represents the number of nodes in the system, and is the sum of N_T, N_L and N_C.

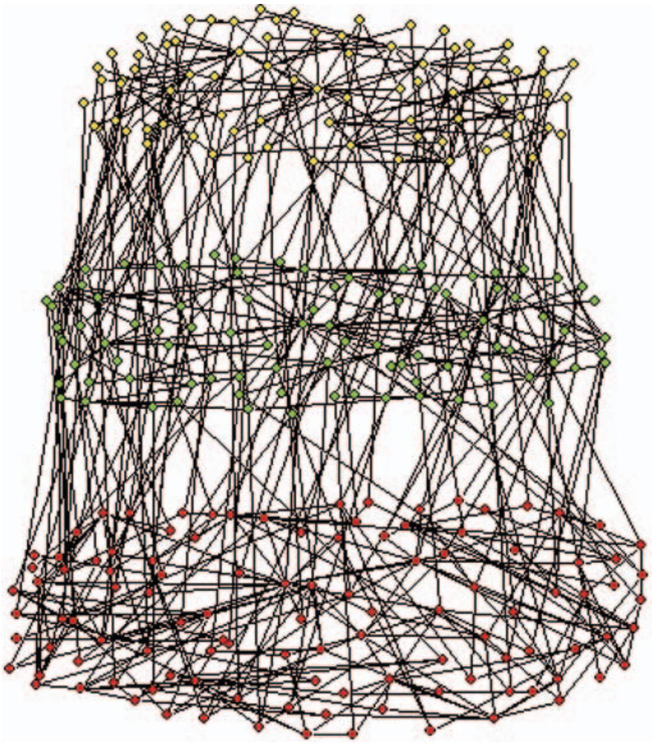


Fig.4 The schematic diagram of multi-layer interdependent network model

3. Attack strategy for structural invulnerability evaluation

3.1 Attack sequence strategy based on node degree

When only partial information about the system can be obtained, for example, the number of command relations or the quantity of communication connections between the communication equipment or the amount of critical traffic nodes, the attack strategy can be formulated according to the degree of node as followed:

$$\beta(i)=\frac{d_i^{\alpha}}{\sum_{i=1}^{N} d_i^{\alpha}} \quad \text{...} \quad (7)$$

In formula (7), d_i represents the degree of network node including command-control node t_i, communication network node l_i and traffic network node c_i. α represents the adjustment parameter of attack sequence strategy. When $\alpha>0$, the greater the degree of node, the greater is the probability of suffering strike. When $\alpha = 0$, each node is attacked with the same probability β = 1/N, which is equivalent to a random attack strategy. When $\alpha<0$, the greater the degree of node, the less is probability of suffering the strike.

3.2 Attack sequence strategy based on node betweenness

When the complete detail of the system can be acquired, the attack sequence strategy can set up based on the node betweenness which means the ratio of the number of lines passing through the node is the total number of the shortest transmission lines in all the shortest transmission lines in the network.

$$B_i=\sum_{j\neq k\neq i}\frac{l_{jk}(i)}{l_{jk}} \quad \text{...} \quad (8)$$

B_i can reflect the global influence of nodes in the whole network. Thus, the probability of a node being attacked can be expressed as equation (9).

$$\eta(i)=\frac{B_i^{\alpha}}{\sum_{i=1}^{N} B_i^{\alpha}} \quad \text{...} \quad (9)$$

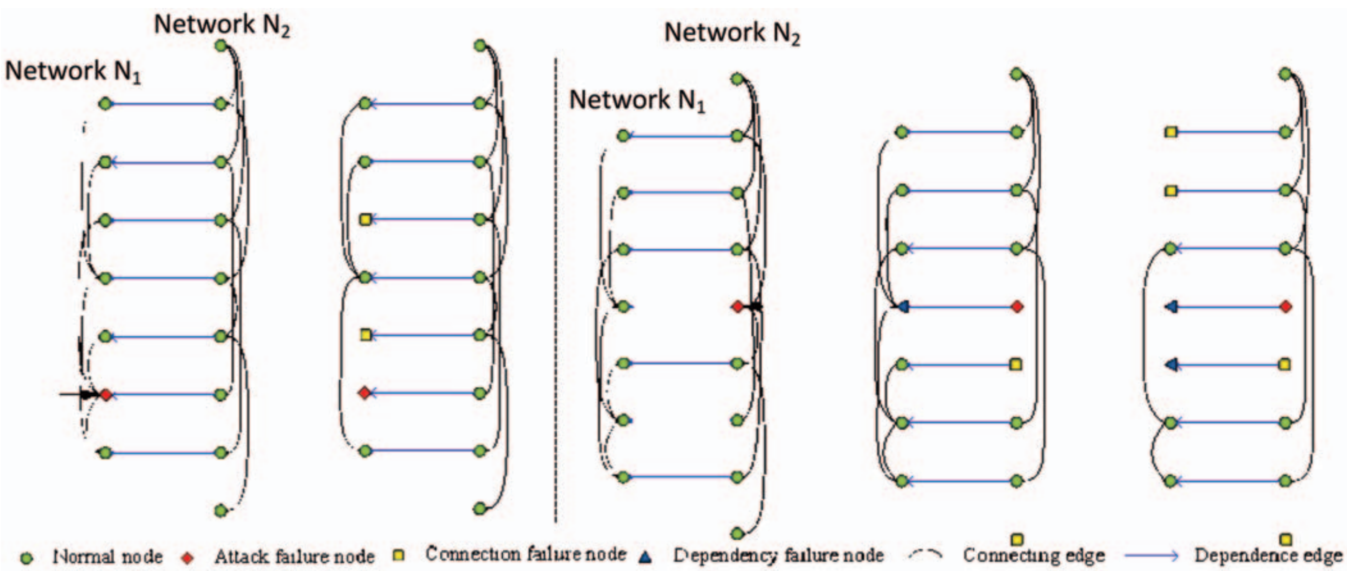
When $\alpha > 0$, the greater the betweenness of a node, the greater is the probability of suffering strike. When $\alpha = 0$, each node is attacked with the same probability η =1/N, which is equivalent to a random attack strategy. When $\alpha<0$, the greater is betweenness of a node, the less is probability of suffering the strike.

4. Failure mechanism of multi-layer emergency logistics system

4.1 Failure propagation process

Failure propagation analysis is the basis of network invulnerability evaluation. Emergency logistics network consists of three layers of basic network, but essentially it has been built up based on the dependency between one layer of network and another. The command-control network is the top-level network. The space communication network is the underlying network relative to the control network. Compared to the physical transportation network, the space communication network is the upper layer network, and physical transportation network is the lower-level network. So, the failure process after the emergency logistics network suffering attacks should be divided into two different models.

Figs.5(a) and 5(b) show the failure propagation process caused by attacking the upper network node. Since the lower layer network has no dependency on the upper layer network,



(a) Initial state (b) Steady state (c) Initial state (d) State 2 (e) Steady state

Fig.5 Cascading failure of interdependent networks the node failure process can only be propagated in the upper layer network. If one node is invalid after suffering a strike, the associated lower-level node becomes connection failure point due to isolated from the effective connected area.

Figs.5(c)-5(e) show the failure propagation process caused by attacking the underlying network node. Since the upper network has dependency on the lower layer network, the node failure process occurred in lower layer network not only propagate in the lower-level network, but also spread to the upper layer network through the multi-layer dependency relationship.

4.2 Failure mechanism algorithm

According to the analysis of failure propagation process about emergency logistics system, shown in Fig.5, the failure mechanism algorithm is obtained as follows:

Step 1: Determine the attack mode, and generate the node attack sequence $\{v_1, v_2, ;;;, v_k\}$ according to the attack strategy;

Step 2: Determine the type of attack node. If it belongs to the command-control network, then go to step 3. If it belongs to the space communication network, then turn to step 4. If it belongs to the physical transportation network, then go to step 5;

Step 3: The attack node v_i belongs to the command-control network, that is to say, $v_i \in V_T$, then remove the node v_i and its connection edge in the command network. Then, remove the associated connection failure points and its edges which are isolated from the effective connected area. Else, turn to step 6;

Step 4: The attack node v_i belongs to the space communication network, that is to say, $v_i \in V_L$, then remove the node v_i and its connection edge in the communication network. Then, remove the associated connection failure points and its edges which are isolated from the effective connected area. Determine whether there is a command node in the command network that is dependent on these failure nodes, if exists, then delete those nodes in command network and turn to step 3, else turn to step 6;

Step 5: The attack node v_i belongs to physical transportation network, that is to say, $v_i \in V_C$, then remove the node v_i and its connection edge in physical transportation network. Then, remove the associated connection failure points and its edges which are isolated from the effective connected area. Determine whether there is a communication node in the space communication network which is dependent on these failure nodes, if exists, then delete those nodes in communication network and turn to step 4, else turn to step 6;

Step 6: Calculate the connectivity of the emergency logistics system after suffering attack.

5. Indicators for structural invulnerability evaluation

The invulnerability evaluation of multi-layer emergency logistics system mainly focus on the influence on whole logistic system after some nodes suffering accidental destruction. The selection or formulation of invulnerability index needs to accord with the emphasis of our research. This paper focuses on the structural invulnerability of the emergency logistics system, thus, the maximum connectivity in the complex network theory can apply to this research.

$$S(i) = \frac{N'(i)}{N} \quad \ldots \quad (10)$$

In equation (10), N is the total number of initial nodes of the logistic network, and N' is the number of nodes that contained in maximum connected group. In order to compare with the previous invulnerability results, this paper propose the effective connectivity indicator which contains all effectively connect logistics area after attack.

$$S'(i) = \frac{N_T^*(i) + N_L^*(i) + N_C^*(i)}{N_T + N_L + N_C} \quad \ldots \quad (11)$$

In equation (11), N_T, N_L, N_C is the total number of initial nodes of command-control network, space communication network and physical transportation network. N^*_T,N^*_L,N^*_C, is the number of connected group nodes that contain valid command object, the traffic line and the communication nodes. The larger value of S', means the larger effective area of the system after attack, thus the better is invulnerability property.

With the increase of number of attacks i, when the number of attacks reach a certain value i_c, the whole system will be completely collapsed, and all nodes in the system are invalid, $S'(i_c)=0$, illustrating i_c is the threshold of system collapse.

6. Numerical experiment

In this paper, a regional emergency logistics system in Sichuan province, China is selected as the object of numerical experiment. And, the multi-layer emergency logistics system model is established according to the modelling method proposed before. Fig.4 shows the topology of this system, where 288 nodes contain, including 80 command nodes, 96 communication nodes, 112 traffic nodes, and 817 sides, including 102 lines of command relation, 180 connections of communication relation, 235 lines of traffic relation, 300 connecting edges between networks.

The ThinkPad T430 computer which is equipped with 4 cores 2GHz processor and 16GB capability of memory has been used as experimental hardware platform, using MATLAB 2016a software for 8 threads parallel computing related procedures. In order to compare with the traditional invulnerability evaluation result based on monolayer network model, the basic model of command control network, information communication network and transportation network are established and calculated.

6.1 Node degree distribution of emergency logistics system

The distribution of the degree can reflect the macro statistical characteristics of a network. In this paper, $P(D)$ has been used to define the degree distribution of network node. The meaning is the proportion of nodes with node degree equal to d in the total number of network nodes. The statistical analysis of the node degree of the emergency logistics system is shown in Fig 6.

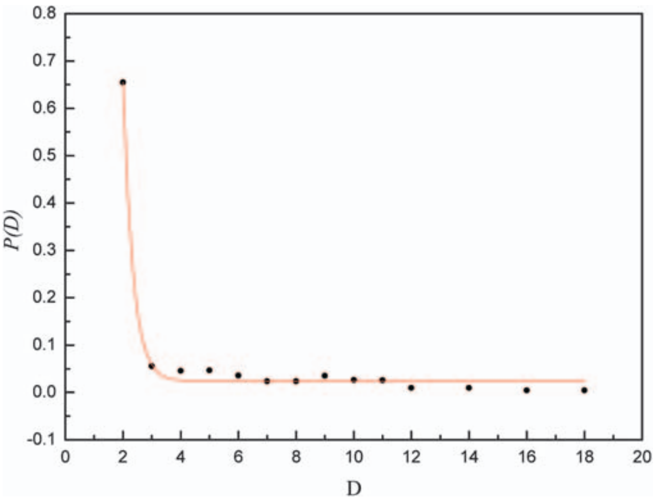


Fig.6 Network node degree and degree distribution probability relation graph

It can be seen from the figure that the number of nodes with node degree below 3 is almost 70%, that is to say, the degree of most nodes is relatively small, which reflects the majority of the commanding organization in command and control network only have limited command relationship. Most of the communication facilities in the information communication network acquired few communication lines and only a small number of traffic nodes located in the key positions. In addition, the node degree distribution curve of the emergency logistics system is similar to the power function, which shows that the node degree distribution of the network conform to the power law distribution approximately, in other words, the network has scale-free characteristics.

In order to further explore the complex network characteristics of the node in emergency logistics system, the node degree and its distribution probability are processed by using double logarithm. The fitting curve results are shown in Fig 7.

The node degree and node degree distribution are handled with double logarithm, and the results are linear regression fitted. The equation of log $(P(D))$ = -0.06776 - 1.77558 log (D) is obtained, and the coefficient of determination is R^2 = 0.82295. The above statistical results show that the emergency logistics system obey power law distribution as a whole, that is to say, the overall network reflects the characteristics of scale-free network.

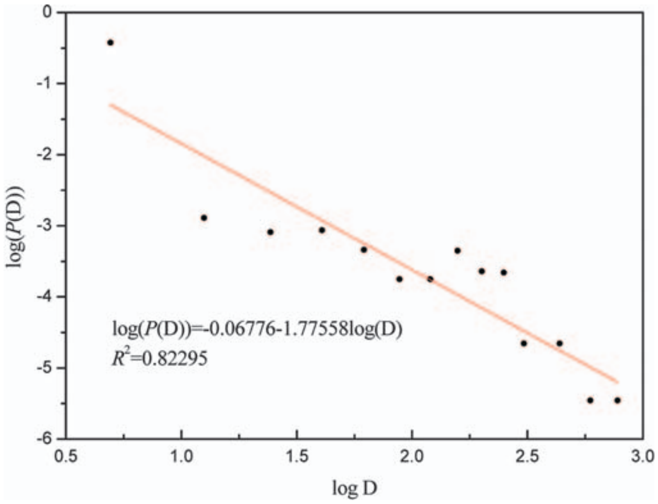


Fig.7 Double logarithmic fitting curve of network node degree and degree distribution

6.2 Structural invulnerability evaluation under intentional attack strategy

Currently, the research on structural invulnerability of emergency logistics system mainly adopts the single-layer command network or transportation network as the research object, that is to say, the network structure of the command-control network or the physical transportation network is used to represent the network structure of the whole emergency logistics network, ignoring the dependence relationship between multi-layer networks.

When the emergency logistic system is suffering intentional attack, the attack order may determined according to the node degree $\{v_1, v_2, ;;;, v_k\}$. And, the command-control network, the information communication network and the transportation network suffered attacks respectively. In order to obtain more reasonable results, the numerical experiment is repeated 200 times, and the average value of each experimental result is regarded as the final result, shown in Fig.8.

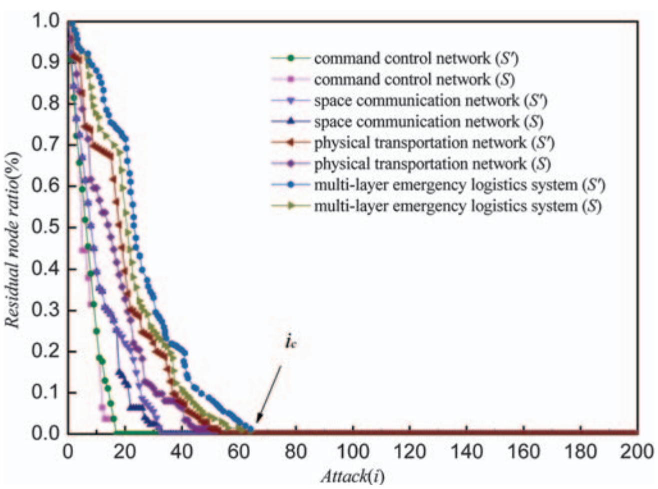


Fig.8 The network invulnerability curve under intentional attack

In Fig.8, when $S \neq 0$, facing with same attack strength, it can always find that $S_T<S_L<S_C<S_E$, $S^*_T<S^*_L<S^*_C<S^*_E$. This conclusion shows that the invulnerability of multi-layer emergency logistics network is superior to that of the single-layer transportation network. The invulnerability of the single-layer transportation is better than that of the single-layer communication network. The single-layer information communication network is superior to the single-layer command control network. The single-layer network model cannot reflect the invulnerability of multi-layer emergency logistics system because of ignoring the interdependence between the networks.

$S_E(i_c = 66) = 0$, indicating that only a selective 54 times attacks can completely make the system paralyzed when the attacker obtain the information about the emergency logistics system accurately. So, it can be concluded that the network is vulnerable to deliberate attacks. Moreover, a comparative analysis of the invulnerability evaluation results based on different evaluation indexes. Moreover, when $S \neq 0$, it always can be found that $S'_T > S_T$, $S'_L > S_L$, $S'_c > S_c$, $S'_E > S_E$, which means that the effective connectivity is greater than the maximum connectivity. This is because the effective connectivity rate taking the nodes which in non-largest effective connectivity group into account. In fact, those nodes are still functional in real system operation.

6.3 Structural invulnerability evaluation under random attack strategy

When the emergency logistic system suffering random attack, the attack sequence determined by system randomly $\{v_1, v_2, ;;;, v_k\}$. Considering the randomness of random attack strategy, the numerical experiment is repeated 200 times as well, and the average value of each experimental result is taken as the calculation result, shown in Fig 9.

In Fig.9, the downward trend of the curve is relatively smooth. When $S \neq 0$, facing with same attack strength, it can always find that $S_T<S_L<S_C<S_E$, $S'_T<S'_L<S'_C<S'_E$., showing that the invulnerability of multi-layer emergency logistics network is superior to that of the single-layer network. $S_E(i_c = 125) = 0$, indicating that the number of attacks must reach 125 times in order to achieve network paralysis effect. It shows that the network reflects strong invulnerability under random attacks. What is more, the similar regular pattern under intentional attack is still obviously in random attack circumstance, which is $S'_T > S_T$, $S'_L > S'_L$, $S'_C > S_C$, $S'_E > S_E$. Thus, the validity of effective connectivity rate is illustrated as well.

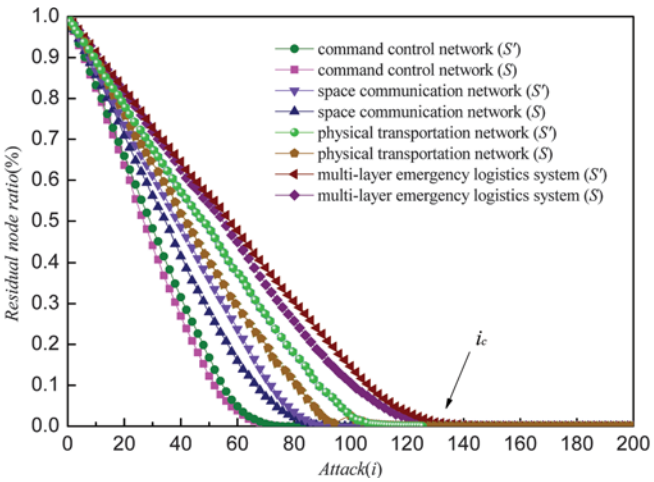


Fig.9 The network invulnerability curve under random attack

7. Conclusion

This paper proposes the complex multi-layer logistic model consists of command-control network, space communication network and physical transportation network based on interdependent network theory. By analyzing the invulnerability result under intentional attack and random attack, the conclusion can draw as follows. Firstly, the three-layer network model of emergency logistics system based on the interdependent network theory is more coincident with the actual situation of system compared to the network model established by traditional single network model. Moreover, the invulnerability analysis method proposed in this paper is more accurate and detailed than the traditional method. The next step in the study is meaningful to extend the single dependency relationship of a node to multiple dependencies, and the invulnerability result can be further optimized.

Acknowledgments

This paper is supported in part by The National Key Technology R&D Program of China (2017YFC0806306), Education Science fund of the Military Science Institute of Beijing, China (No.2016JY481), and Chongqing Graduate Scientific Research Innovation Project, China (No.CYB17148).

References

1. Barabasi, A. L. and Albert, R. (1999): "Emergence of Scaling in Random Networks." *Science*, 286(5439): 509.
2. Chen, C. X. and Wang, Y. K. (2012): "The Invulnerability of Emergency Logistics Network Based on Complex Network [M]//LUO *J. Affective Computing and Intelligent Interaction*. 2012: 789-+.
3. Guo, J., Han, Y., Guo, C., Lou, F. and Wang, Y. (2017): "Modeling and Vulnerability Analysis of Cyber-Physical Power Systems Considering Network Topology and Power Flow Properties." *Energies*, 10(1): 1-21.
4. Holme, P., Kim, B. J., Yoon, C. N. and Han, S. K. (2002): "Attack vulnerability of complex networks." *Physical Review E Statistical Nonlinear & Soft Matter Physics*, 65(2): 56-109.
5. Hong, J. D., Jeong, K. Y. and Xie, Y. C. (2015): "A multi-

objective approach to planning in emergency logistic network design." *International Journal of Industrial Engineering – Theory Applications and Practice*, 22(4): 412-425.

6. Huang, L., Wang, W. and Wang, M. G. (2013): "Simulation Research of Space-Time Evolution of Emergency Logistics Network Reliability Based on Complex Network Theory." *Discrete Dynamics in Nature and Society*, (3): 399-412.
7. Kuhnle, A., Nguyen, N. P., Dinh, T. N. and Thai, M. T. (2017): "Vulnerability of clustering under node failure in complex networks." *Social Network Analysis & Mining*, 7(1): 8.
8. Li, X. H. and Tan, Q. M. (2011): "Hierarchical Traffic Network Design under Emergency Logistics [M]// Zhang, H., Shen, G., Jin, D." *Advanced Research on Information Science, Automation and Material System*, Pts 1-6. 2011: 732-735.
9. Wang, J. J., Jiang, C. X., Gao, L. X., Yu, S., Han, Z. and Ren, Y. (2016): IEEE Complex Network Theoretical Analysis on Information Dissemination over Vehicular Networks [M]. 2016 IEEE International Conference on Communications. 2016.
10. Watts, S. H. and Strogatz, D. J. (1998): "Collective dynamics of 'small-world' networks." *Nature*, 393(6684): 440-442.