A Combined Routing Path and Node Importance Network Invulnerability Evaluating Method for Ad Hoc Network

Weiling Zhou, Bo Li, Zhongjiang Yan(✉), and Mao Yang

School of Electronics and Information,
Northwestern Polytechnical University, Xi'an, China
2018261692@mail.nwpu.edu.cn, {libo.npu,zhjyan,yangmao}@nwpu.edu.cn

Abstract. In this paper, a new network invulnerability evaluation model based on routing path and node importance is proposed. The core of the invulnerability algorithm lies in two levels, comprehensive consideration of the influencing factors of network to point-to-line network invulnerability. The algorithm considers the influence of the proportion of important nodes of the network on the invulnerability of the network, and considers the influence of the number of paths between the communication nodes on the invulnerability of the path. Through simulation comparison, it is found that this algorithm improves the sensitivity of network invulnerability to the number of paths, and is suitable for communication networks in the case of multiple routing paths.

Keywords: Network invulnerability · Routing path · Node importance · Ad hoc network

1 Introduction

Ad hoc network is a network system that is interconnected or organized by a communication node in a system through a distributed protocol without a backbone network. As a distributed, temporary autonomous multi-hop network, the ad hoc network itself does not have a fixed infrastructure. In the network, each user terminal can generate and process some business data for other users like a host. The terminal can also be like a router, establish and maintain a network topology, and implement some routing protocols [1,2]. Since wireless communication is limited by distance, if two user equipments that are far apart from each other want to communicate with each other, they must use some intermediate users located between their geographical locations to forward information for them, thereby realizing user communication [3].

Ad hoc networks are characterized by topological dynamics [4,5], limited link bandwidth, time-varying capacity, limited node energy, short network lifetime, and limited physical security [6,7]. Ad hoc networks are often used to secure information in harsh environments such as battlefields and natural disasters.

D.-J. Deng et al. (Eds.): WiCON 2019, LNICST 317, pp. 20–33, 2020.
https://doi.org/10.1007/978-3-030-52988-8_3

The transmission task, therefore, puts high demands on the invulnerability of the network structure [8].

The study of network invulnerability is extremely important for complex networks [9,10]. In a broad sense, it refers to the ability of a network to maintain its normal operating state after encountering a fault or being attacked [11]. In a narrow sense, network invulnerability means that after a network encounters a random failure or an external attack, there is also a connected area in the network that is proportional to the total node of the network [12,13]. There are three types of attacks in the network: one is man-made destruction, with a strong purpose, and priority attacks on important nodes. The second is natural disasters, large-scale node damage in an area [14,15]. The third is a random failure.

Invulnerability is the ability of a network to continue its function when a node [16,17] or edge in the network fails due to its own cause or by intentional attacks from the outside world. Node connectivity, network communication efficiency, and network average node degree are usually used as measures to measure network invulnerability. Based on these network invulnerability measures, Feng H, Li C and Xu Y proposed an invulnerability assessment algorithm based on temporal networks [18]. However, the algorithm can not reflect the impact of routing path resistance. In view of its failure to comprehensively evaluate the network invulnerability measure and node importance, this paper proposes an invulnerability algorithm based on link and node importance. The algorithm can well reflect the impact of the proportion of important nodes and the number of routing paths.

This article will first introduce and analyze some important measures of network system model and network invulnerability in the second section, and briefly describe the existing methods of invulnerability assessment. Then the third section details the principle and definition of the invulnerability algorithm based on link and node importance. The fourth section carries out simulation results and performance analysis and the fifth section summarizes the full text.

2 System Model

2.1 Network Model and Invulnerability Measure

There are two common network models: random networks and scale-free networks. In a random network, each pair of nodes in the network is always connected with a certain probability. Therefore, the number of nodes that each node can communicate in a random network is roughly the same, but the network topology constructed at this time is very complicated. As the number of nodes in the network increases, the number of connections that can exist increases, and the probability of node connections decreases exponentially. Therefore, random networks are also called index networks. In most real-world application networks, not all nodes are completely in the same state. There will always be some nodes that have a large degree of connectivity, while others have a small degree of connectivity, and usually they account for 2:8. A network with this characteristic is called a scale-free network.

The invulnerability measures are divided into non-topological measures and topological measures. The core idea of non-topological measures is to select network simple attributes that are independent of the network topology as a measure of the network's ability to resist damage. Common network attributes include the number of remaining available nodes, coverage area, network lifetime, and so on. These network attributes are simple and easy to obtain. In many literatures, one or several network attributes are often used as indicators of the measure of invulnerability. However, network attributes are difficult to fully and accurately reflect the network's anti-destructive performance. When designing the invulnerability algorithm, the most used is the topological measure of invulnerability.

The network topology can be mathematically represented by graph theory, that is, graph $G = (V, E)$. Suppose the graph is an undirected weightless graph, where $V = (v_1, v_2, v_3, ..., v_n)$ is a set of all nodes, $E = (e_1, e_2, e_3, ..., e_n)$ is a collection of all edges (network links) of the network topology. Here are a few important topological measures for analyzing invulnerability [19]:

The Importance of the Node. In the network model, especially the scale-free network model, the importance of the node in the network topology is often evaluated by the degree and the median, and the greater the degree and the medium, the more important the node is. The importance of a node reflects the importance of the node in the overall network topology and is an assessment of the importance of the nodes in the network topology. The impact of a critical node being destroyed on network invulnerability is much greater than that of a normal node.

The Degree of the Node. In the network, the number of edges k_i of the node v_i is called the degree of the node v_i. The greater the degree of a node, the more important it is in the network. The average of the network is:

$$k = \frac{1}{N} \sum_{j=1}^{N} k_i \tag{1}$$

The Median of Nodes. The median B_i of the node v_i is the sum of the proportion of the number of nodes passing through the shortest path in the network. If the minimum distance between a pair of nodes N_{jk}, and $N_{jk}(i)$ paths pass through node v_i, then v_i contributes to $N_{jk}(i)/N_{jk}$ for the pair of nodes, and node v_i The contributions to all pairs of nodes are added together to get the median B_i of the node v_i, namely:

$$B_i = \sum_{j,k \in V j \neq k} \frac{N_{jk}(i)}{N_{jk}} \tag{2}$$

The Critical Point Removal Ratio f_c. When a node in the network is attacked and the network is at the edge of the crash, the number of nodes attacked on the network as a percentage of the total number of nodes is called the critical point removal ratio, which is recorded as f_c.

Maximum Connectivity S. The ratio of the number of nodes in the largest connected branch in the network to the total number of nodes in the network is called the maximum connectivity, namely:

$$S = \frac{m(G)}{N} \tag{3}$$

It can be seen from the above equation that $0 \leq S \leq 1$, and if and only if the network is fully connected, there is $S = 1$; If and only if the network completely crashes, there is $S \approx 0$, that is, all nodes in the network are isolated nodes after being attacked.

Global Efficiency E. First use d_{ij} as the shortest distance between any two nodes v_i and node v_j in the network. Define the average value of the network global efficiency as the sum of the reciprocal of the shortest distance between any two nodes in the network topology, as follows:

$$E = \frac{1}{N(N-1)} \sum_{j,k \in V j \neq k} \frac{1}{d_{ij}} \tag{4}$$

This paper will focus on the scale-free network model, especially in the case of some network routes supporting multiple paths, to carry out research on network invulnerability.

2.2 Existing Invulnerability Assessment Method

In this section, an existing network invulnerability assessment method based on dynamic network model will be introduced. First explain some basic indicators of the temporal network, then describe how to use these measures to quantitatively define the non-destructibility of the temporal network [18].

Temporal Network Model. At time t, the network topology is modeled as $G(t) = (V(t), E(t))$. The network topology consists of two important factors, where $V(t)$ represents the set of vertices and $E(t)$ represents Edge set. $E(t) = e_{ij}(t)$, if the distance $d_{ij}(t)$ between the two nodes is less than the shortest communication distance, then $e_{ij}(t)$ exists.

Temporal Distance. The shortest time distance $d_{ij}(t_1, t_2)$ can be defined as the minimum time distance among the lengths of all time paths between the nodes v_i and v_j in the time window $[t_1, t_2]$. During the time window $[t_1, t_2]$, the average time distance $L(t_1, t_2)$ of a given topology model G is defined as:

$$L(t_1, t_2) = \frac{1}{N(N-1)} \sum_{j,k \in V j \neq k} d_{ij}(t_1, t_2) \tag{5}$$

Time Global Efficiency. Time efficiency means that there is a lack of path between a longer time path and a node that is simultaneously disconnected in time. The time global efficiency $E(t_1, t_2)$ of a given topology model G is:

$$E(t_1, t_2) = \frac{1}{N(N-1)} \sum_{j,k \in V j \neq k} \frac{1}{d_{ij}(t_1, t_2)} \tag{6}$$

Invulnerability Algorithm Definition. Use $\Delta E(G, D)$ to indicate that the efficiency loss on the time graph G caused by the node damage D is $\Delta E(G, D) = E_G - E_{G_D}$, then the network invulnerability R_G of the topology map G against the node damage D is defined as:

$$R_G = \frac{\Delta E(G, D)}{E_G} = 1 - \frac{E_{G_D}}{E_G} \tag{7}$$

It is easy to know from the above analysis that the invulnerability algorithm introduced in this section mainly depends on the shortest distance between two communication nodes, but does not fully consider the impact of other network invulnerability measures against destructiveness. It can be known from the definition of invulnerability that the network can still maintain the communication function when the node or edge of the network is damaged due to its own or external factors. The shortest distance of the communication link involved in the above-mentioned invulnerability algorithm can be regarded as the invulnerability of the network, but it does not reflect the invulnerability of the nodes in the network. Therefore, this invulnerability algorithm is not comprehensive.

3 Invulnerability Algorithm Based on Link and Node Importance

In the network invulnerability assessment, the analysis of the importance of the node is a very important part. The existing network invulnerability evaluation model fails to comprehensively evaluate the network invulnerability measure and the importance of the node. In this section, A new invulnerability algorithm is proposed based on the multi-index evaluation method of link invulnerability and node importance, considering the influence of the invulnerability R of the

invulnerability data link network in the network. The following network invulnerability R is defined as:

$$R = k \times R_{side} + (1 - k) \times R_{node}, 0 \leq k \leq 1 \tag{8}$$

It can be seen from the above equation that the network invulnerability is determined by two aspects: one is the invulnerability of the end-to-end routing path; the other is the influence of the nature of the nodes in the network on the network invulnerability. The influence factor k is used to determine the degree of influence of these two parameters against destructiveness. The following will specifically analyze the invulnerability of the end-to-end routing path and the impact of network node resistance.

3.1 Invulnerability Calculation Method

Path Invulnerability Calculation. R_{side} is used to indicate the invulnerability of the end-to-end routing path, which is the average value of end-to-end communication invulnerability between all two nodes s and t in the network topology, as follows:

$$R_{side} = \frac{\sum_{s=1}^{M} \sum_{t=1, t \neq s}^{M} R(s,t)}{\sum_{s=1}^{M} \sum_{t=1, t \neq s}^{M} 1} \tag{9}$$

Where M represents the total number of nodes in the network. $R(s,t)$ is the end-to-end communication invulnerability measure between two nodes s, t. When there are multiple routing paths between two nodes, the path with the highest invulnerability in the path is selected to represent the current two. End-to-end communication intrusion between communication nodes, namely:

$$R(s,t) = max(r_1, r_2, r_3, ..., r_N) \frac{N}{N + C}, 0 \leq C \leq 1 \tag{10}$$

N indicates the total number of routing paths between the specified nodes s and t, and C is a parameter indicating the degree of influence of the number of paths against the destructiveness, and takes values between 0 and 1. r_n represents the invulnerability of the n-th routing path between the node s and the node t, which is a function of the path hop count α, the probability of the intermediate node being damaged β, and the intermediate link interruption probability γ, ie

$$r_n = f(\alpha, \beta, \gamma) \tag{11}$$

And r_n is negatively related to these three factors. For example, the invulnerability is negatively correlated with the number of hops of the path. When the number of hops of the path is increased, the probability that the intermediate node is damaged or the intermediate path is interrupted will be larger, and the invulnerability of the path will be lower. In the process of network communication, nodes are generally transmitted with a shortest path. The more hops, the

worse the reliability of the path, and the worse its invulnerability. Because the link or node may be invalid due to external factors, if there are multiple shortest paths between the nodes, the data may be transmitted by other shortest paths after a shortest path fails.

After considering these influencing factors, define the invulnerability of a single path:

$$r_n = \prod_{i=0}^{K}(1 - P_i) \tag{12}$$

Where K is the hop count of the routing path and P_i is the probability of the interruption of the i-th intermediate link (i-th hop) in the routing path. It is easy to see that in this definition, when the K value is larger, the more hops of a single routing path, the lower the invulnerability of the path will be, so the path invulnerability and the hop count of the path have a negative correlation.

In the communication network, the outage probability of the link is proportional to the packet loss rate of the link. The packet loss rate is used to indicate the outage probability of the intermediate link:

$$P_i = P_{max}\frac{d_i}{D_{max}} \tag{13}$$

Where d_i represents the distance length of the i-th intermediate link in the current routing path, and D_max represents the longest link distance between two nodes that can communicate. P_max represents the packet loss rate when the two nodes are apart from D_max, and theoretically takes the parameter $P_max = 0.1$.

In summary, the average end-to-end invulnerability in the network topology is:

$$R_{side} = \frac{\sum_{s=1}^{M}\sum_{t=1,t\neq s}^{M} max(r_1, r_2, r_3, ..., r_N)\frac{N}{N+C}}{\sum_{s=1}^{M}\sum_{t=1,t\neq s}^{M} 1}, N \geq 1, N \in Z, M \in Z \tag{14}$$

$$r_n = \prod_{i=0}^{K}(1 - P_{max}\frac{d_i}{D_{max}}), K \geq 1, K \in Z \tag{15}$$

Node Invulnerability Calculation. At the same time, for the scale-free network model, the "importance" of a node is related to its position in the network path. A few nodes often have a large number of connections. These nodes with high degrees and median are important nodes in the network. For example, the cluster head in the clustering topology, the multi-hop relay node (MPR) in the OLSR protocol, and the like. From the perspective of the overall topology of the network, the stability of the network structure also depends on the proportion of important nodes in the network.

$$R_{node} = \frac{Number\ of\ important\ nodes}{Total\ number\ of\ network\ nodes} \tag{16}$$

The destruction of important nodes has a greater impact on the network topology than the destruction of general nodes. When there are redundant important nodes, the destroyed path will make it easier to find alternative paths, thus improving the overall network invulnerability.

3.2 Algorithm Innovation

Consider Multiple Paths. The target algorithm only considers the shortest distance between two nodes, which is equivalent to considering a single routing path for communication between two nodes. The newly defined invulnerability algorithm fully considers the invulnerability of multiple paths.

$$R(s,t) = max(r_1, r_2, r_3, ..., r_N)\frac{N}{N+C}, 0 \leq C \leq 1 \tag{17}$$

In the definition of the above formula, the parameter C is used to adjust the degree of influence of the number of paths against the damage. When the value of C is larger, the influence of the change of the number of paths on the network invulnerability is greater.

Network invulnerability is defined as "the ability of the entire network to complete the transmission of business information after the destruction of some nodes in the network." The network completes the transmission of service information, mainly relying on the routing path between the source end node and the destination end node. Therefore, analyzing the impact of node destruction on the number of network routing paths can be found to include the following two cases:

All routing paths are lost: If some of the critical nodes in the network are damaged, the routing path between the source node and the destination node is completely disconnected and does not exist, it can be considered that "the network is damaged by this part of the node" And a network crash occurs;

The number of routing paths is reduced: some links are disconnected and the path through the link is lost due to node destruction, thereby reducing network invulnerability; for example, two paths are required to transmit the same information before the node is damaged (thus Reduce the impact of the node due to packet loss), but now due to the destruction of a node, only one path can be used to transmit the message, so the network invulnerability is reduced.

The new invulnerability formula shows that the invulnerability is positively correlated with the number of paths between the two nodes. When there are more alternative paths between the two nodes, the invulnerability is higher.

Consider All Nodes. The target algorithm only considers the nodes that can communicate with each other, and does not consider nodes that are isolated and cannot communicate. The newly defined invulnerability algorithm takes into account not only all nodes in the network.

$$R_{side} = \frac{\sum_{s=1}^{M}\sum_{t=1,t\neq s}^{M} R(s,t)}{\sum_{s=1}^{M}\sum_{t=1,t\neq s}^{M} 1} \tag{18}$$

It also considers the impact of the nature of the nodes in the network on the overall network invulnerability:

$$R_{node} = \frac{Number\,of\,important\,nodes}{Total\,number\,of\,network\,nodes} \tag{19}$$

In this algorithm, the degree of the node, that is, the number of edges associated with the node, is used to determine whether the node is an important node. In the case of a known network topology, the number of important nodes in the network can be determined, thereby obtaining the influence of the nature of the nodes in the network on the network invulnerability.

4 Performance Analysis of Invulnerability Algorithm

4.1 Performance Trends for Different Link Distances

When the original algorithm calculates invulnerability, only the shortest distance between two nodes is considered, which is equivalent to considering a single routing path for communication between two nodes. The newly defined invulnerability algorithm fully considers the invulnerability of multiple paths. The following simulation graph abscissa is the number of routing paths that can exist between two communication nodes set in the routing protocol, and the ordinate is the invulnerability R of the network. It can be seen that the original algorithm calculates the network invulnerability without the routing path. The number of bars affects, while the new invulnerability formula shows that the

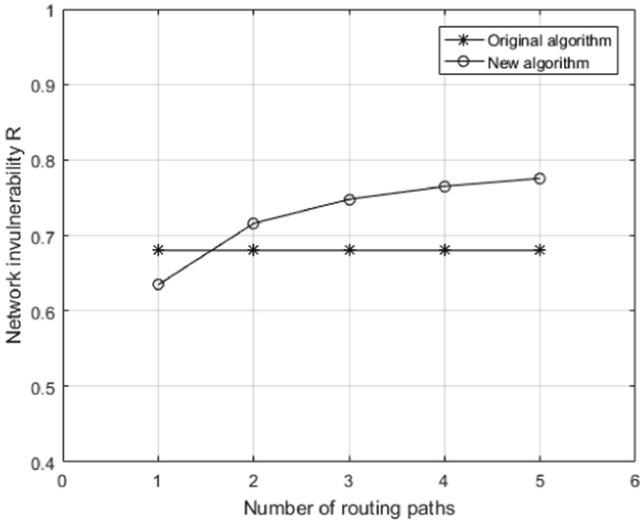

Fig. 1. Comparison between original algorithm and new algorithm when path number changes

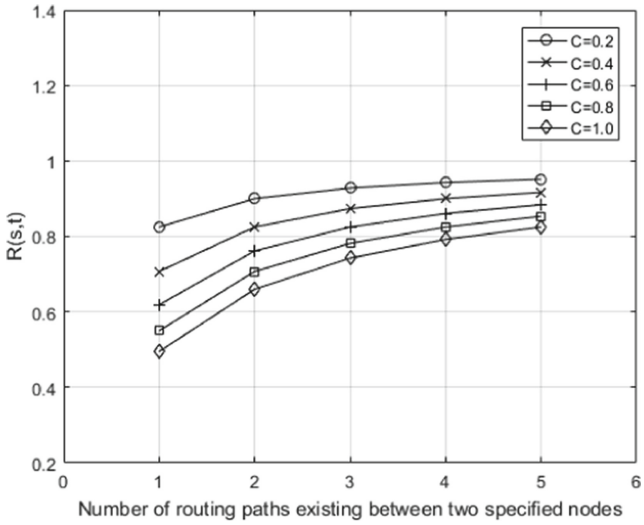

Fig. 2. The relationship between the new algorithm and the number of routing paths

invulnerability is positively related to the number of paths between two nodes, that is, when there are more alternative paths between the two nodes, the higher the invulnerability. This performance is also in line with actual communication.

In order to study the relationship between the newly proposed network invulnerability measurement algorithm and the number of routing paths, the impact of the number of routing paths on the end-to-end communication invulnerability can be analyzed.

The horizontal coordinate of the above figure is the number of routing paths existing between two communication nodes, and the ordinate is the end-to-end path invulnerability $R(s,t)$ between the two communication nodes. The parameter C is used to indicate the degree of influence of the number of paths against the damage, and the value is between 0 and 1. It can be found from the above figure that when the fixed parameter C is constant, as the number of communication routing paths between two nodes increases, the invulnerability becomes larger. With the increase of C value, the influence of the number of paths on the path invulnerability is more and more obvious, and the curvature of the curve is larger (Figs. 1 and 2).

It can be proved that the newly proposed invulnerability algorithm is applicable to multipath routing networks. Because in the routing protocol, when two designated nodes communicate with each other, the more recorded paths, when the network link is damaged, other alternative links can be found for information transmission without causing two nodes. Inter-communication is interrupted, and the path invulnerability will be relatively large. This is consistent with our simulation results of invulnerability analysis.

The path invariance algorithm is applied to the dynamic source routing protocol (DSR) to study the effectiveness of the network invulnerability algorithm. DSR is a routing protocol used in the Mobile Ad Hoc Network (MANET). It works in the Internet layer of the TCP/IP protocol suite and is a simple and efficient routing protocol designed for multi-hop wireless Ad Hoc networks. In the DSR routing protocol, a specified number of routing paths can be set and recorded. Therefore, in this paper, the number of different routing paths can be set under the DSR routing protocol, and the following figure can be simulated (Fig. 3).

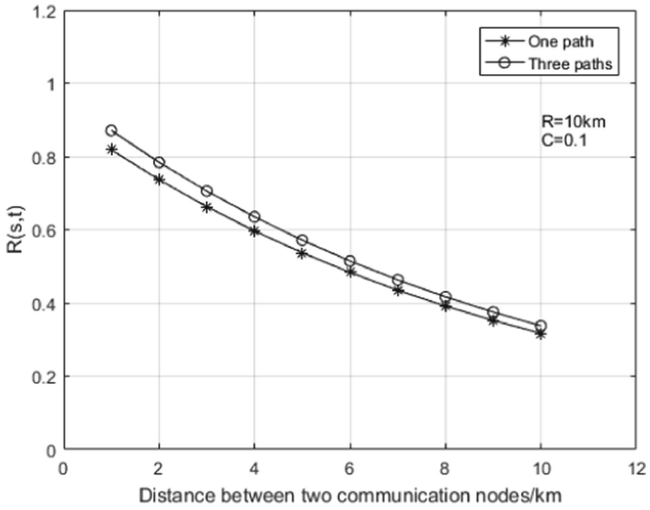

Fig. 3. Invulnerability of the same route under different path number settings, C = 0.1

The abscissa of the above figure is the physical distance between two communication nodes, and the ordinate is the end-to-end path invulnerability $R(s,t)$ between the two communication nodes. First, we can see that as the physical distance between two communication nodes increases, the path invulnerability continues to decrease. Moreover, a DSR routing protocol with three routing paths is always more invulnerable than an DSR routing protocol with only one path. However, the sensitivity of the two routing protocols to the number of paths is controlled by parameter C.

Study the effect of the distance between two communication nodes and the maximum transmission distance against destruction (Figs. 4 and 5):

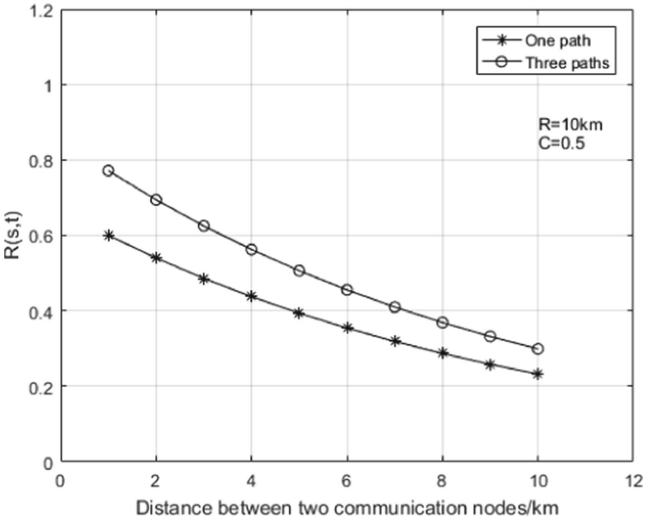

Fig. 4. Invulnerability of the same route under different path number settings, C = 0.5

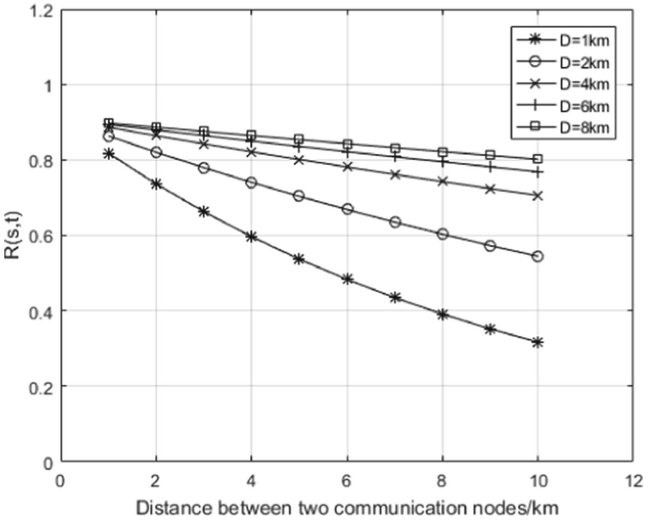

Fig. 5. Relationship between invulnerability and node distance and maximum communication distance

The abscissa of the above figure is the physical distance between two communication nodes, and the ordinate is the end-to-end path invulnerability $R(s,t)$ between the two communication nodes. Analysis shows that when the maximum transmission distance between two communication nodes is fixed, such as when D = 1 km, as the distance between two communication nodes increases, the path

invulnerability is continuously reduced, which is related to the actual situation. It is consistent. As the communication path increases, the link is more likely to be damaged due to its own or external elements. The increased probability of the link being destroyed will increase the probability of the interruption of the routing path, which in turn will lead to a decrease in the path invulnerability of the network.

The maximum transmission distance between two communication nodes also has an impact on the destructiveness. The smaller the maximum transmission distance, the lower the path resistance of the network. This is because the maximum transmission distance becomes smaller, which may lead to an increase in the number of hops of the node communication path, and more intermediate nodes, so that the probability of the node being damaged on the communication link increases, and the probability of interruption of the sub-link increases. Thus, the path of the mentor network is reduced.

5 Conclusion

This paper focuses on the research of self-organizing network invulnerability. Firstly, it introduces two common network topology models: random network and scale-free network, and analyzes some important topological network invulnerability measures. Aiming at the problem that the existing network invulnerability evaluation model fails to comprehensively evaluate the network invulnerability measure and node importance, a new network invulnerability evaluation algorithm based on link and node importance is proposed. The algorithm can reflect the influence of the number of routing paths and the degree of importance of network nodes. Through simulation verification, it is also found that the algorithm can correctly and effectively reflect the influence of node communication distance and maximum transmission distance on network invulnerability.

Acknowledgement. This work was supported in part by the National Natural Science Foundations of CHINA (Grant No.61771392, 61771390, 61871322, 61501373 and 61271279), the National Science and Technology Major Project (Grant No. 2015ZX03002006-004 and 2016ZX03001018-004), and Science and Technology on Avionics Integration Laboratory (Grant No. 20185553035).

References

1. Li, K., Wang, H.: Research on invulnerability of scale-free network with a unified method. Int. J. Arts Technol. **11**(3), 266–284 (2019)
2. He, S., Jin, C., Wei, H., Liu, Q.: A measure method for network invulnerability based on improved albert algorithm. In: International Conference on Instrumentation (2011)
3. Albert, R., Jeong, H., Barabasi, A.L.: Error and attack tolerance of complex networks. Nature **340**(1), 378–382 (2000)
4. Fu, X., Yao, H., Yang, Y.: Exploring the invulnerability of wireless sensor networks against cascading failures. Inf. Sci. (2019)

5. Wen, C., Zhang, X.: The invulnerability of robust communication network. In: IEEE International Conference on Communication Software & Networks (2016)
6. Luo, J.-J., Feng, Y.-H., Zuo, C.: Analysis on the invulnerability of network based on scale-free network, pp. 1519–1522 (2018)
7. Rao, Y.P., Lin, J.Y., Hou, D.T.: Evaluation method for network invulnerability based on shortest route number. J. Commun. **30**(4), 113–117 (2009)
8. Yun, F., Hong, L.Z., Hai, T.Y.: Research of new certain metrics of network invulnerability. Adv. Mater. Res. **301–303**, 1322–1326 (2011)
9. Li, E., Gong, J., Huang, J.: Analysis about functional invulnerability of convergent network based on function chain. Binggong Xuebao/Acta Armamentarii **40**(7), 1450–1459 (2019)
10. Zhao, D.J., Yang, H.T., Jian, J., Yu, H.: Modeling and simulation of the invulnerability of space information network. In: International Conference on Internet Technology & Applications (2010)
11. Peng, K., Huang, B.: The invulnerability studies on data center network. Int. J. Secur. Appl. **9**(11), 167–186 (2015)
12. Tian, X.W., Liu, S.Y., Zhang, Z.H., Dong, H.J.: A topology optimal algorithm for improving the invulnerability of scale-free networks. In: International Conference on Information System & Artificial Intelligence (2017)
13. Bao, X.-C., Dai, F.-S., Han, W.-Z.: Evaluation method of network invulnerability based on disjoint paths in topology. Xi Tong Gong Cheng Yu Dian Zi Ji Shu/Syst. Eng. Electron. **34**(1), 168–174 (2012)
14. Chen, H.-H., Lin, A.-M.: Complex network characteristics and invulnerability simulating analysis of supply chain. J. Netw. **7**(3), 591–597 (2012)
15. Wu, J., Tan, S.-Y., Tan, Y.-J., Deng, H.-Z.: Analysis of invulnerability in complex networks based on natural connectivity. Complex Syst. Complex. Sci. **11**(1), 77–86 (2014)
16. Jiang, L., Zhang, F., Yang, R., Xu, K.: Influence of sensor nodes on the invulnerability of tree network. Telkomnika (Telecommun. Comput. Electron. Control) **13**(4), 1242–1250 (2015)
17. Fu, X., Li, W., Fortino, G.: Empowering the invulnerability of wireless sensor networks through super wires and super nodes, pp. 561–568 (2013)
18. Feng, H., Li, C., Xu, Y.: Invulnerability analysis of vehicular ad hoc networks based on temporal networks. In: IEEE International Conference on Computer & Communications (2017)
19. Feng, H.-F., Li, C.-H.: Invulnerability analysis of vehicle self-organizing network based on complex network. Comput. Appl. **36**(7), 1789–1792 (2016)