Applied Mathematics and Computation 366 (2020) 124636

Contents lists available at ScienceDirect

Applied Mathematics and Computation

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

Robustness of multi-agent formation based on natural connectivity

ZhengHong Deng*, Jiwei Xu, Qun Song, Bin Hu, Tao Wu, Panfei Huang

School of Automation, Northwestern Polytechnical University, Xi'an 710072, China

ARTICLE INFO

Article history:
Received 28 May 2019
Revised 28 June 2019
Accepted 29 July 2019
Available online 24 September 2019

Keywords:
Multi-agent
Robustness optimization
Topology
Natural connectivity
Chaotic genetic algorithm

ABSTRACT

The robustness of multi-agent topology has great importance to the design of multi-agent formation, while to improve the robustness of the topology without increasing its cost is also very important. In this paper, we proposed an optimization method for the robustness of multi-agent formation. The natural connectivity is used for measuring the robustness of multi-agent formation. Through analysis, the formation optimization problem is transformed into a 0–1 nonlinear programming problem. In order to solve the problem quickly, the paper presents a genetic algorithm based on chaotic search optimization. When the method given in this paper is applied to specific requirements, only the constraint conditions need to be modified, so the method has good universality. The results show that the optimized network can significantly improve the robustness of the network.

1. Introduction

With the development of science and technology, multi-agent cooperative has become the most popular technology. The robustness of multi-agent topology becomes an important premise and foundation, as it is an important part of the cooperative control for multi-agents. Currently, the connectivity of the topology is widely considered at the beginning of system design. However, for most of the systems, the tolerability of the topology is still very low, e.g., the World Wide Web [1,2] and the Internet [1], etc., exhibit low robustness under malicious attacks. For multi-agent systems, the topology could be fail because of random attacks or malicious attacks to some nodes or edges, which could result in system crash. There are many possible which could cause these attacks, such as natural disasters, the failure of electronic components, and malicious attacks by hackers or enemy and so on. Therefore, it is important to ensure that the system topology is more robust when designing multi-agent formations, especially for the multi-agent system working in harsh environments or military tasks. It is very important to ensure that the entire formation is still working when some nodes are under attack.

At present, the research on the robustness of complex networks mainly focuses on the empirical study of robustness, robustness modeling analysis and robustness optimization. In the empirical study of robustness, the robustness of the World Wide Web [1], web network structure [3], protein network [4], Internet [5], P2P shared network [6] has been studied by malicious attacks and random attack. As more attention is paid to the study of complex networks [7–10], these studies give useful suggestions for improving the robustness of the network.

Based on the empirical research, some researchers have modeled and analyzed the robustness of complex networks, and tried to give the measurement criteria and indicators of network robustness. Cohen et al. [11] proposed the critical node

* Corresponding author.
E-mail address: dthree@nwpu.edu.cn (Z. Deng).

https://doi.org/10.1016/j.amc.2019.124636
0096-3003/

deletion ratio, and then extended this theory to the malicious attack situation [12]. Gallos et al. [13] studied attack strategies and defense strategies that depend on the degree of network node. Vazquez and Moreno [14] studied the robustness of arbitrary degrees of networks. Sun et al. [15] studied the statistical properties of evolutionary networks, and the responses of these networks to both random and malicious attacks.

Robust modeling and analysis of complex networks provides a theoretical basis for optimization of networks. Therefore, various methods for optimizing the robustness of the network have been proposed, with various starting point. In [16], different network models are constructed for robustness optimization. The network robustness is studied from the characteristics of network non-uniformity in [17–20], and the robustness is optimized by applying joint entropy [17], degree distribution entropy [18], structural entropy [19], and distributed normalized entropy [20]. In [21], the network robustness is improved by adding points, edges, or reconnecting network points and edges. In [22–24], the network robustness is improved by hiding network information or hiding part of the network. In summary, the essence of network robustness optimization is the game [25–29] between network structure and attack strategy.

However, to the best of our knowledge, there is no study devoting to optimizing network robustness from the perspective of cost in the literature. To improve network robustness without increasing network costs is very important for many application scenarios, such as multi-agent formation. In the multi-agent formation, the nodes of the network (the number of multi-agents) and the edge of the network (the communication connection between the agents) are fixed. Increasing the number of nodes and edges will increase the cost of the formation, while the extra cost will be too expensive to be accepted.

In this paper, a network robustness optimization method by optimizing the network at a fixed cost (fixed network nodes and fixed network edges) is proposed, and the robustness of the formation is improved in our experiment. In our experiment, the topology characteristics of the optimized network are analyzed, and it is found that the nodes with greater degrees tend to connect with each other, thus forming a group structure. Malicious attack and random attack experiments were carried out on the optimized network and the BA network, and the experiment result showed that the optimized network had better robustness without increasing the network cost.

2. Optimization model

Wu et al. [30] believe that network robustness results from the redundancy of the connected links between any two nodes in the network. In other words, the more links between nodes in the network, the stronger the robustness of the network. They proposed natural connectivity as a measure of network robustness. Natural connectivity has proven to be a significant advantage both in computational complexity and for measuring robustness [30]. Therefore, in this paper, natural connectivity is used as the objective function for network robustness optimization. The natural connectivity is defined as:

$$\bar{\lambda} = In\left(\frac{1}{N}\sum_{i=1}^{N} e^{\lambda_i}\right) \tag{1}$$

Here: λ_i is the ith element in the set of eigenvalues $\{\lambda_1,\lambda_2,\lambda_3,\ldots, \lambda_N\}$ of the adjacency matrix, and $\lambda_1 > \lambda_2 > \lambda_3 > \cdots > \lambda_N$.

A multi-agent topology is essentially a graph, expressed as $G(V, E, A)$. Here, $V = (v_1,v_2,\ldots, v_N)$ is the set of vertices of the graph G, and $|V|=N$; $E = (e_1,e_2,\ldots, e_W)$ is the set of edges of the graph G, and $|E|=W$; A is the adjacency matrix of graph G, and $A(G) = (a_{ij})_{N\times N}$. Before optimizing the multi-agent topology, we need to make the following constraints:

A. *Simple graph constraints.* In the multi-agent formation discussed in this article, it is assumed that the weights of the agents are consistent and the connections are undirected. Therefore, the elements of the adjacency matrix A need to satisfy the following conditions:

$$\begin{cases} a_{ij} = 0 \, or \, 1 \\ a_{ij} = a_{ji} \\ a_{ii} = 0 \end{cases} \tag{2}$$

B. *Degree not 0 constraint.* In a multi-agent formation, it is assumed that each agent is directly or indirectly connected to other agents, and the formation will never actively discard the agent:

$$k_i > 0, i = 1, 2, 3, \ldots, N \tag{3}$$

Here, k_i is the degree of the node v_i.

C. *Cost constraints.* In a multi-agent formation, the number of edges can be seen as the cost of the network, or as the cost for constructing multi-agent formation. Therefore, from the perspective of multi-agent formation networking costs, it is obviously that the more connections there are in G, the higher the cost is. Assuming that the total number of edges of the multi-agent formation is constant, that is to say, only the 0-order distribution characteristics of the complex network are considered.

$$\sum_{i=1}^{N}\sum_{j=1}^{N} a_{ij} = 2W \tag{4}$$

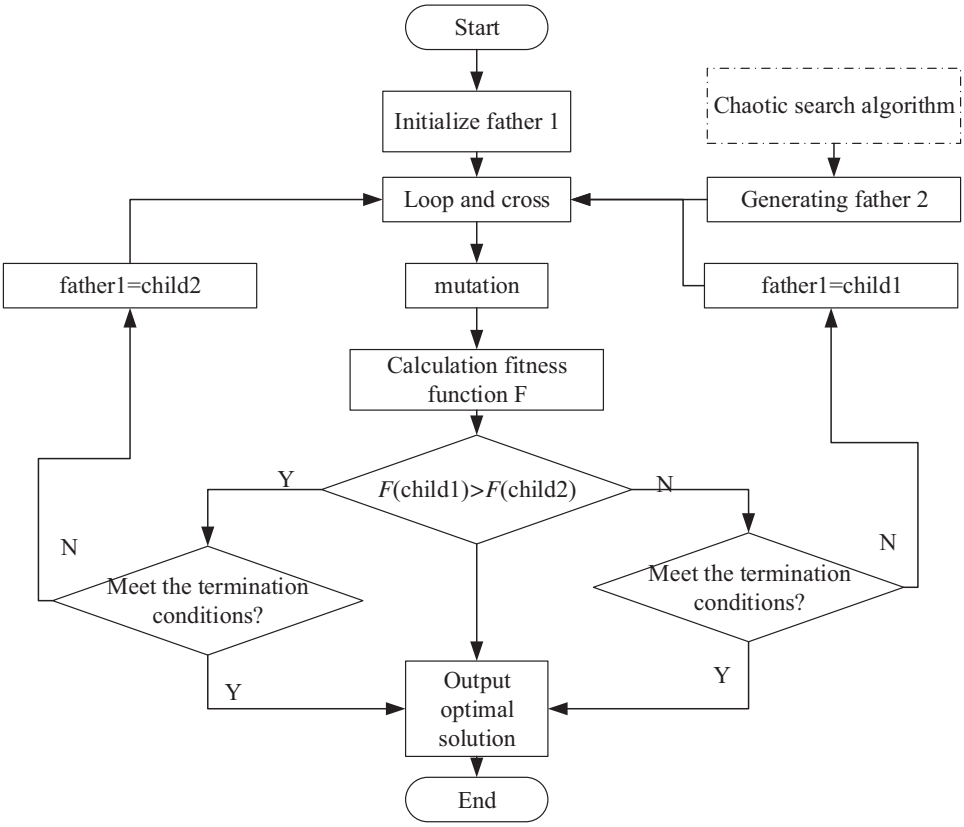


Fig. 1. The process of chaotic genetic algorithm.

Under this scenario, the constraint can be written as:

$$\max \bar{\lambda} = In\left(\frac{1}{N}\sum_{i=1}^{N} e^{\lambda_i}\right)$$
$$s.t.\begin{cases} a_{ij} = 0 \text{ or } 1 \\ a_{ij} = a_{ji} \\ a_{ii} = 0 \\ k_i > 0 \\ \sum\sum a_{ij} = 2W \end{cases} \tag{5}$$

Through modeling analysis, the topology optimization problem is transformed into combination optimization problem. For different real-life applications, by utilizing different constraint parameters according to the application, the model can be applied to its topology optimization problem, which suggests the strong universality of the proposed model.

3. Chaotic genetic algorithm

To improve the accuracy and speed of model solving, we use chaotic search algorithm to optimize genetic algorithm, and improve the accuracy by power function carrier.

3.1. The general mentality of chaotic genetic algorithm

At this stage, there are many ways for solving 0–1 integer programming. However, when the problem size is large, the computation of the general method will be very heavy, and the entire solution process will be very difficult or even impossible to carry out. Chaos is the most common phenomenon in nonlinear systems, and it has the characteristics of randomness, regularity and ergodicity. Therefore, the chaos search genetic algorithm is used for the solution of the optimization model. The solution process is shown in Fig. 1.

In the algorithm, the generation of the father2 is the optimal solution obtained by the chaos algorithm. The optimal solution has the following characteristics: first, to ensure the quality of the population; second, to ensure the diversity and randomness of the population. When chaotic search is applied into genetic algorithm, it can ensure that the offspring have higher fitness, so that the population could evolve continuously, and the convergence is avoided to avoid local optimum. For an N-dimensional optimization problem, it is equivalent to finding a point in the N-dimensional space that maximizes or minimizes the objective function. Therefore, it is equivalent to giving N chaotic variables as a spatial coordinate. Since each component space is inside [0, 1], it exhibits a highly dense feature, and each coordinate component has a correlation. The resulting point is able to traverse all the points of the dimension unit hypercube to achieve a global search. However, as the complexity of solution space increases, chaotic search cannot guarantee the speed and accuracy of the search. In order to improve the ergodicity of chaotic variables, and to improve the efficiency and accuracy of chaotic optimization, a new carrier method is proposed.

3.2. Optimization of power function carrier

Consider logistic mapping, i.e.:

$$g: z_{k+1} = \mu * z_k(1 - z_k) \tag{6}$$

In this formula, μ represents the control parameter. When $\mu = 4$, the chaotic invariant set of g is [0, 1], and the system is chaotic under this condition. Logistic maps have ergodicity, however, the ergodicity is not strong enough. In order to improve the ergodicity of the Logistic map, it is necessary to reduce the probability density of the Logistic map orbit. Therefore, the density at both ends of the interval is reduced, and the probability density in the interval is increased. Following this idea, the following carrier mode is adopted.

$$z'_k = \begin{cases} z_k^u, z_k \in (0, a] \\ z_k, z_k \in (a, b] \\ z_k^v, z_k \in (b, 1] \end{cases} \tag{7}$$

In this formula, we have $0 < a < b < 1$, $0 < u < 1$, $1 < v$. It can be inferred from the formula that firstly, with the decreasing of u and the increment of v, the distance of point movement will be farther; secondly, there is still ergodicity in [0, 1]. Therefore, the chaotic search algorithm can be described as the following:

Step 1: Using the sensitivity of the chaotic variable, assigning different initial values to the following formula:

$$z_{i,k+1} = \mu * z_{i,k}\left(1 - z_{i,k}\right) \tag{8}$$

Here, the value of chaotic fixed points should not be assigned.

Step 2: Dividing the [0, 1] interval according to the count of variables, and setting number to it.

Step 3: Updating the value of z'_k following formula (7).

Step 4: Determining the interval of the generated chaotic variable:

$$x_{ij}(k) = \begin{cases} 1, & \text{The } i\text{th variable is in the } j\text{th interval} \\ 0, & \text{The } i\text{th variable is not in the } j\text{th interval} \end{cases} \tag{9}$$

Step 5: Computing the objective function following formula (5). Initially, let $T^* = T(0)$, $x_{ij}^* = x_{ij}(0)$. If $T(k) < T^*$, then keep $x_{ij}(k)$, and let $T^* = T(k)$, $x_{ij}^* = x_{ij}(k)$; otherwise give up $x_{ij}(k)$.

Step 6: Determining whether the termination condition is satisfied. Terminating iteration if the termination condition is satisfied; and going to step 1 otherwise.

4. Numerical results

4.1. Experimental setting

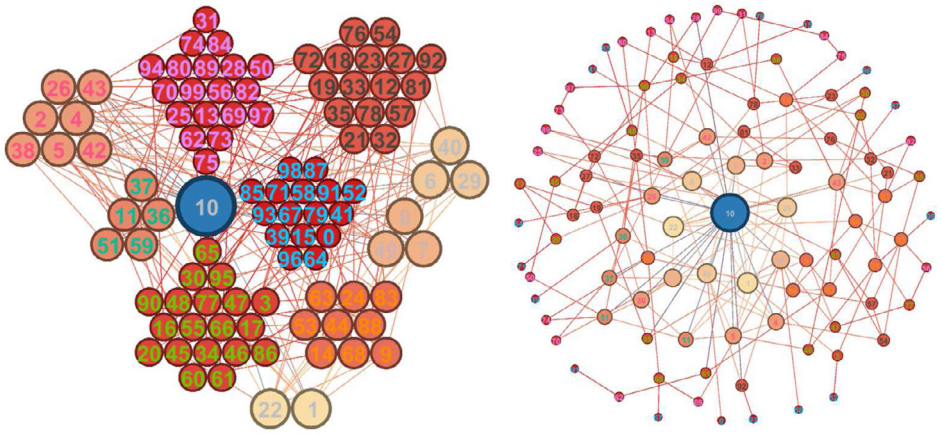
Experimental parameters

Let us consider a scenario in which there is 100 multi-agents in the multi-agents formation, and 196 edges among these agents. For the purpose of fast convergence, the BA network is used for population initialization. In the iterative process, the individual gene length is set to $100^*(100–1)/2 = 4950$, the number of species is set to 10 times the gene length, the crossover probability is set to 0.8, the mutation probability is set to 0.05, and the number of iterations is set to 300 and represented by *iter*. In the iterative process, the exchange principle and the protection degree distribution principle are used in order to satisfy the constraint.

Measurement of robustness

In general, for complex networks, the maximum connected subgraph is used to measure the robustness of the network [1]. Therefore, the robustness indicator S is expressed as:

$$S = \frac{N_{\max}}{N} \tag{10}$$



(a) Optimization network layout Circle Pack Layout and degree as Hierarchy

(b) Optimization network layout similar onion-like

Fig. 2. Topology optimization results.

Here, N represents the number of all nodes in the initial network, and $N_{\max}$ represents the maximum number of subgraph nodes after the attack.

It can be seen that $N_{\max}$ is proportional to S, and the larger $N_{\max}$ is, the more robuster the network is.

4.2. Optimization result analysis

Fig. 2 shows the network after optimization. Fig. 2(a) uses Circle Pack Layout and degree as Hierarchy. Fig. 2(b) is based on the Fruchterman Reingold graph layout algorithm.

As can be seen from Fig. 2, compared with the BA network, in the optimized network, nodes which have larger degree tends to be connected to each other. Therefore, the optimized network presents a group structure. In this experiment, because the average degree of the network is small, the network presents a group structure, and the rest of the nodes are connected almost following the sequence from nodes with larger degree to nodes with smaller degree. In [31], robust networks have a novel 'onion-like' topology consisting of a core of highly connected nodes hierarchically surrounded by rings of nodes with decreasing degree. Compared with the onion-like network in [31], although optimized based on different measures, the two optimized networks exhibit similar structural characteristics. E.g., nodes with large degrees in both networks tend to be connected to each other, and nodes with similar degrees tend to be connected to each other. Therefore, the assortativity coefficient and clustering coefficients of the network could be increased by optimization, which is also observed in our network topology analysis experiments, as shown in Fig. 3 and Fig. 4, respectively. In addition, as the robustness measurement used in this paper is different from the one used in [31], the optimization results could not be completely consistent.

Fig. 3 shows the relation between *iter* and $\bar{\lambda}$ during the simulation. As it is shown in Fig. 3, with the incensement of *iter*, the value of $\bar{\lambda}$ increases, thus verifying the feasibility and effectiveness of the proposed method. In the simulation process, $\bar{\lambda}$ grows fastly in the early stage, and it's grow rate slows down as the *iter* increases. This means that the algorithm converges, and the results tend to be steady.

Fig. 4 shows the variation between the natural connectivity change and the assortativity coefficient during the optimization process. The assortativity coefficient is defined following formula (11).

$$r = \frac{\frac{\sum_k u_k v_k}{W} - \left[\frac{\sum_k \frac{1}{2}(u_k+v_k)}{W}\right]^2}{\frac{\sum_k \frac{1}{2}(u_k+v_k)}{W} - \left[\frac{\sum_k \frac{1}{2}(u_k+v_k)}{W}\right]^2} \tag{11}$$

Here, u_k and v_k represents the degree of the nodes at each ends of an edge, and k represents the degree of the agent node. When $r > 0$, the network is considered to be isomorphic; when$r < 0$, the network is considered to be heterogeneous.

As shown in Fig. 4, with the increment of $\bar{\lambda}$, the network's r is also increasing. This means that the points with larger degrees in the multi-agent formation are more likely to be connected to other points with larger degrees. The nodes in the multi-agent formation tend to be connected with similar nodes, and the conclusion is similar to that of Herrmann et al. [31].

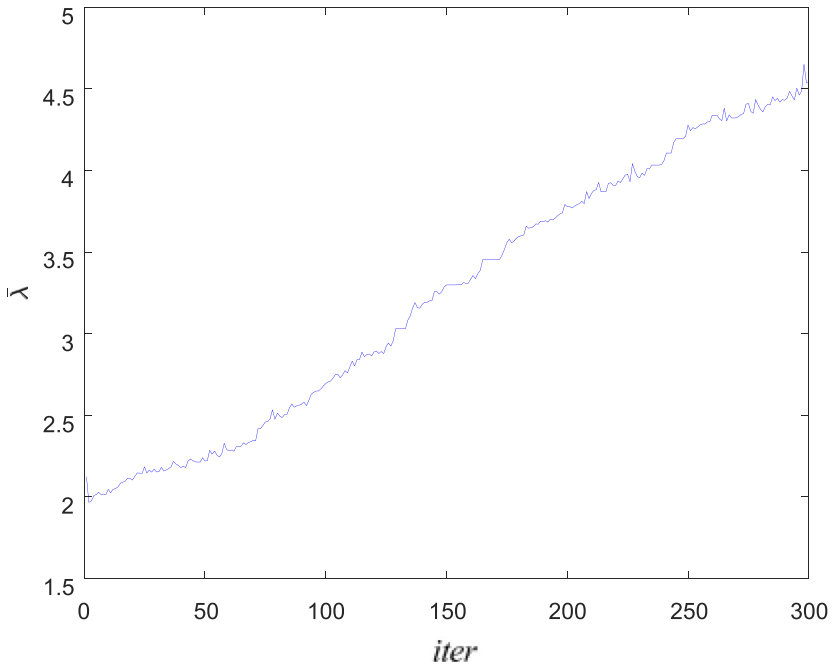


Fig. 3. How does $\bar{\lambda}$ change with increasing of *iter*.

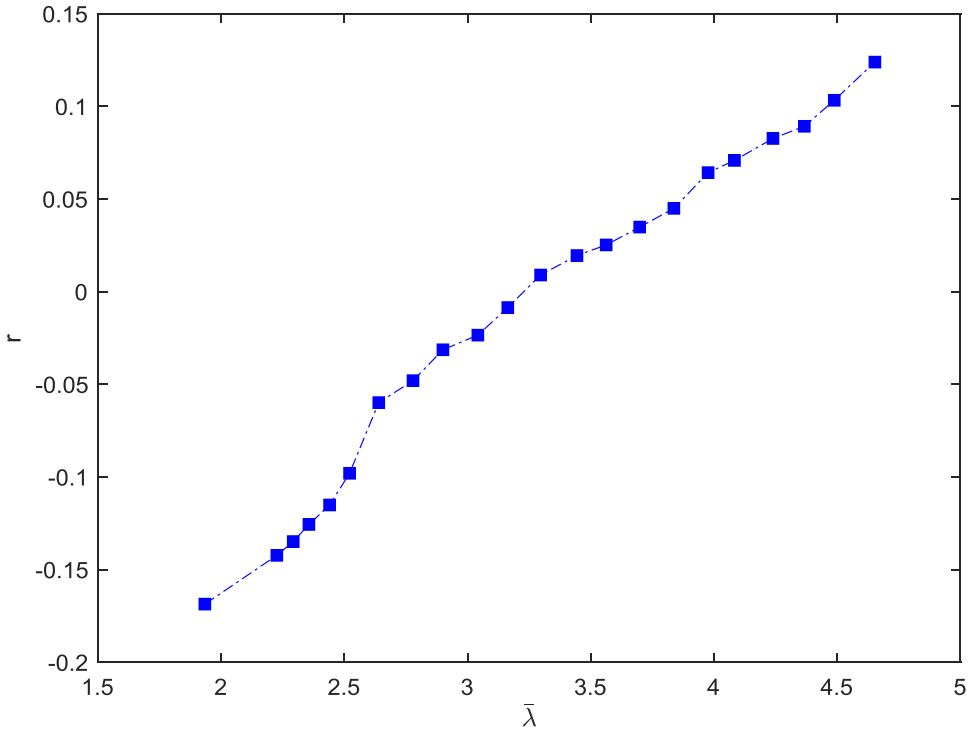


Fig. 4. How does r change with increasing of $\bar{\lambda}$.

Fig. 5 shows the relationship between $\bar{\lambda}$ and multi-agent formation clustering coefficients C during the optimization process. The clustering coefficient is defined as:

$$C = \frac{\sum_{i=1}^{N} C_i}{N} \tag{12}$$

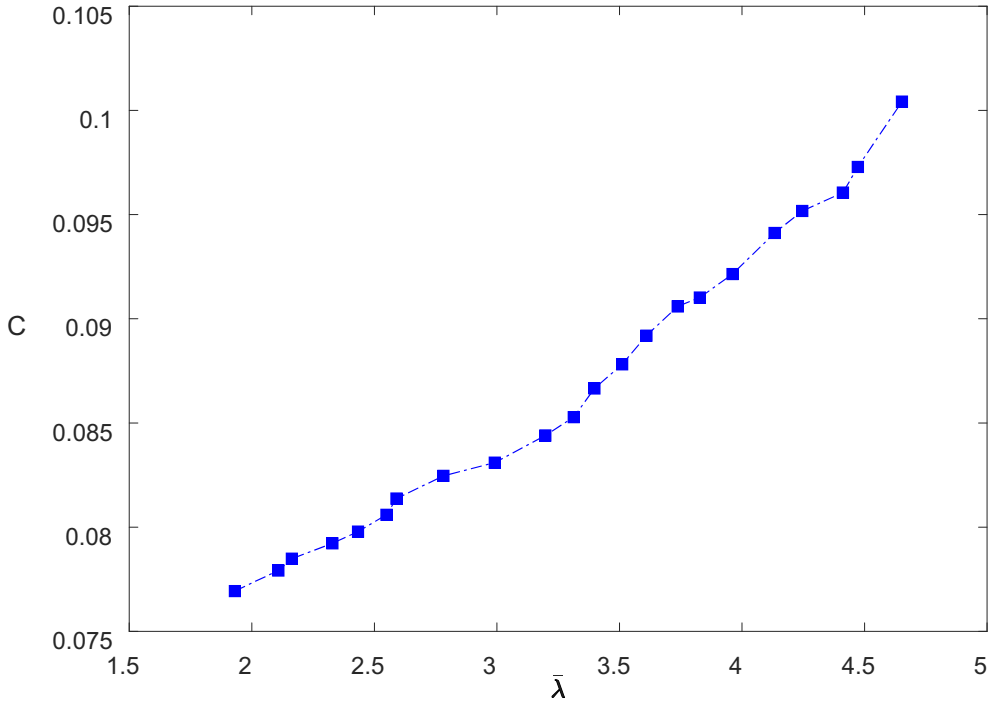


Fig. 5. How does C change with increasing of $\bar{\lambda}$.

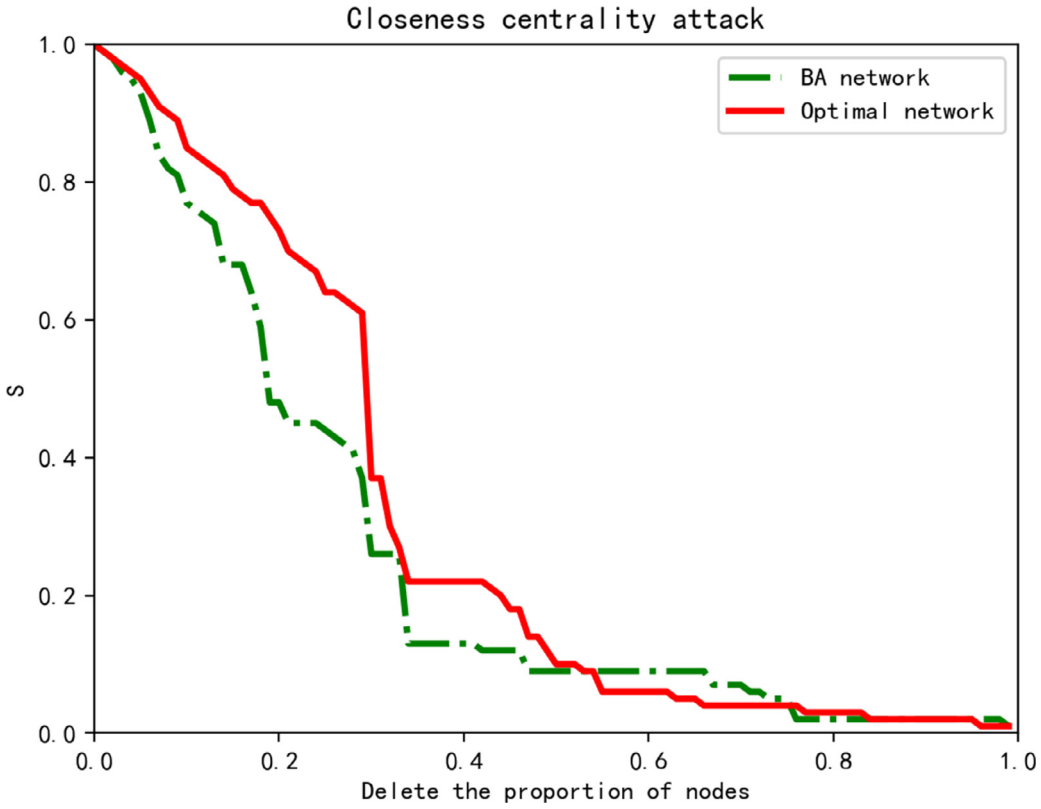


Fig. 6. The results of closeness centrality attack.

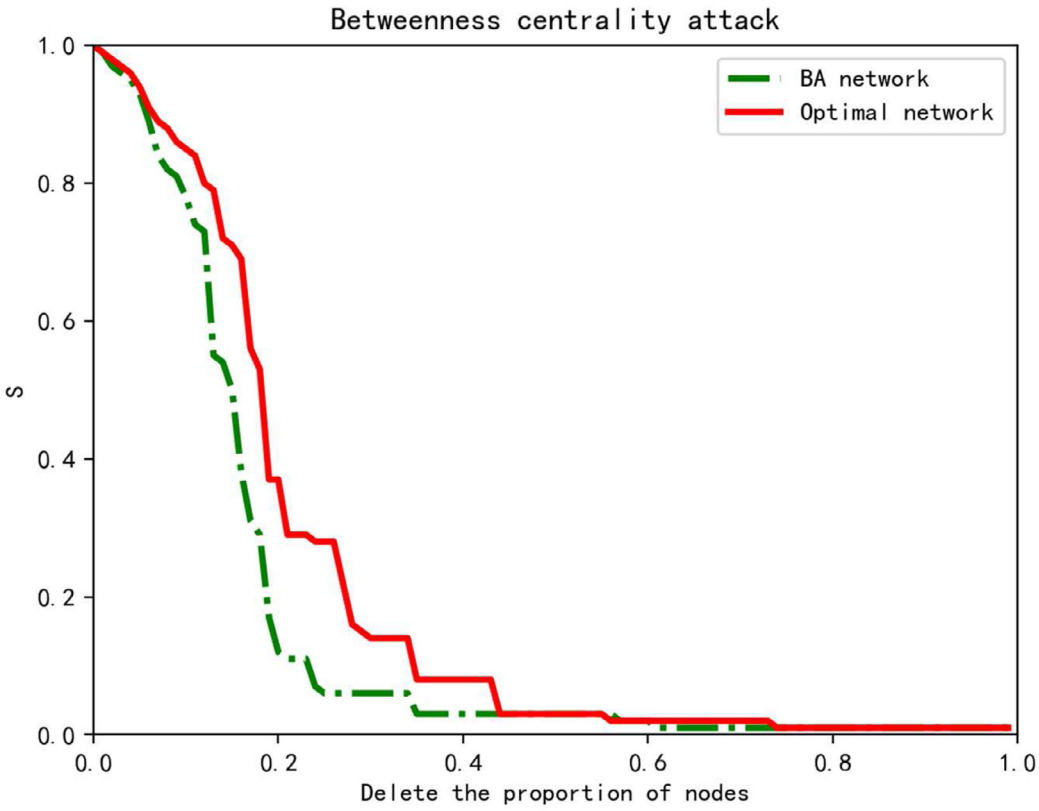


Fig. 7. The results of between centrality attack.

Here, C_i represents the clustering coefficient of node i, which is defined as:

$$C_i = \frac{2E_i}{k_i(k_i - 1)} \tag{13}$$

In formula (12), E_i represents the actual number of edges that exist among the neighbors of node i, and k_i represents the degree of node i.

As shown in Fig. 5,C of the multi-agent formation increases with the increment of, although the improvement is not obvious at some points. This means that in multi-agent formation, nodes tend to build a tight organizational structure, which further suggests that the clustering coefficients of multi-agent formations increase with the increment of robustness.

4.3. Robustness verification

In the robustness analysis, we will use the BA network as a comparison, as the BA network is used for initialization. Both the optimized network and the BA network have 196 edges and 100 vertices. In this experiment, in order to obtain the optimal network optimization result, no limitation is set to the parameter *iter*. However, the termination condition is set to the difference among the optimal fitness of the 50th generation, and the global optimal is less than 10^{-6}. The best optimal network is chosen from 10 optimizations. The malicious attacks includes the closeness centrality attack [32], the between centrality attack [33], the degree attack [34], and the random attacks, with the result of the attack shown in Fig. 6, Fig. 7, Fig. 8, and Fig. 9, respectively.

As can be seen from Fig. 6, when the proportion of deleted nodes is between 53% and 73%, the robustness of the BA network is better than that of the proposed optimized network. However, in the rest of the scale range, the robustness of the proposed optimized network is better than that of the BA network. As can be seen in Figs. 7 and 8, the robustness of the optimized network is always better than the BA network.

As can be seen in Fig. 9, under random attack, the robustness of the optimized network in the range of 54−80% is slightly lower than that of the BA network. In the rest of the range, the robustness of the optimized network is better than that of the BA network.

In summary, for three malicious attack and random attack, the robustness of the optimized network is much better than that of the BA network. The optimization algorithm proposed in this paper could help to improve the robustness of topology for multi-agent network.

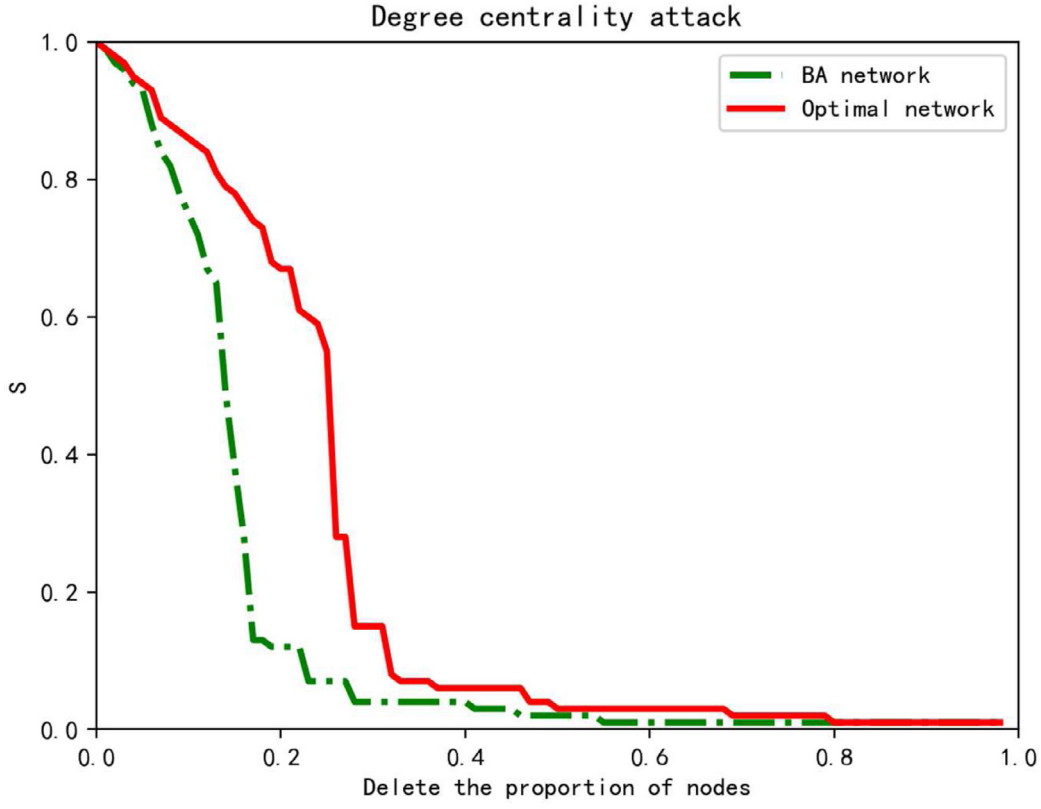


Fig. 8. The results of degree attack.

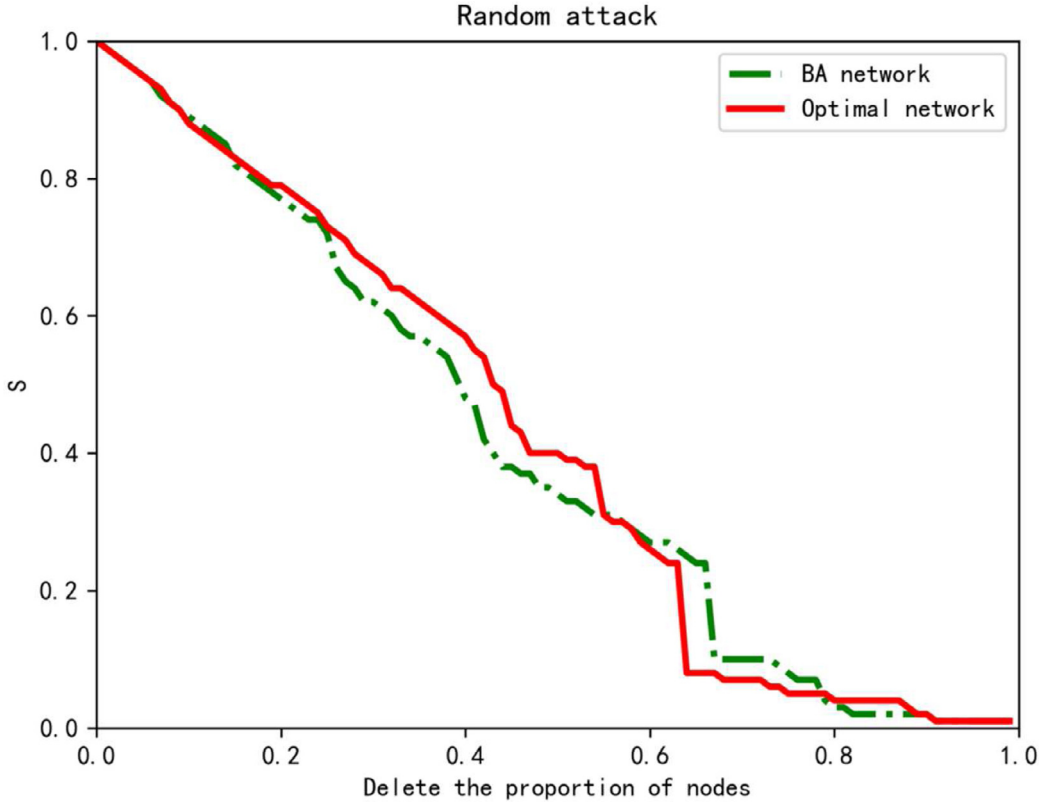


Fig. 9. The results of random attack.

5. Conclusion

To improve the robustness of formation without increasing the cost, an optimization method of multi-agent formation robustness based on natural connectivity is proposed in this paper. Firstly, the robustness optimization model based on natural connectivity is established, and the limitation assumption is designed to the model. Then, the model solving method based on chaotic inheritance is given. Finally, the optimization network optimization process and optimization results are given through experimental simulation. On one hand, through the analysis of the optimized network topology indicators, it is shown that the nodes with larger degrees tend to connect with each other, thus forming a group structure. On the other hand, the effectiveness of the proposed optimization algorithm is verified by comparing the robustness of the network with the BA network under malicious attacks and random attacks.

Acknowledgment

This research was supported by the Shaanxi Key Research and Development Program (2017ZDXM-GY-139). This support is greatly appreciated and it will not lead to any conflict of interests regarding the publication of this manuscript. In addition, the author(s) declare(s) that there is no conflict of interest regarding the publication of this paper.

References

[1] R. Albert, H. Jeong, A.L. Barabasi, Attack and error tolerance in complex networks, Nature 406 (2000) 387–482.
[2] H. Jeong, S.P. Mason, A.L. Barabasi, Z.N. Oltvai, Lethality and centrality in protein networks, Nature 411 (6833) (2001) 41–42.
[3] A. Broder, R. Kumar, F. Maghoul, et al., Graph structure in the web, Comput. Netw. 33 (2000) 309–320.
[4] M.E.J. Newman, S. Forrest, J. Balthrop, Email networks and the spread of computer viruses, Phys. Rev. E 66 (3) (2002) 035101.
[5] D. Magoni, Tearing down the Internet, IEEE J. Sel. Areas Commun. 21 (6) (2003) 949–960.
[6] K. Samant, S. Bhattacharyya, Topology, search, and fault tolerance in unstructured P2P networks, in: Proceedings of the 2004 Hawaii International Conference on System Sciences, IEEE Press, Hawaii, 2004.
[7] P. Zhu, X. Wang, S. Li, Y. Guo, Z. Wang, Investigation of epidemic spreading process on multiplex networks by incorporating fatal properties, Appl. Math. Comput. 359 (2019) 512–524.
[8] P. Zhu, X. Song, L. Liu, et al., Stochastic analysis of multiplex Boolean networks for understanding epidemic propagation, IEEE Access 6 (2018) 35292–35304.
[9] C. Liu, C. Shen, Y. Geng, et al., Popularity enhances the interdependent network reciprocity, New J. Phys. 20 (12) (2018) 123012.
[10] D. Zhao, L. Wang, Z. Wang, et al., Virus propagation and patch distribution in multiplex networks: modeling, analysis, and optimal allocation, IEEE Trans. Inf. Forensics Secur. 14 (7) (2018) 1755–1767.
[11] R. Cohen, K. Erez, D. ben-Avraham, S. Havlin, Resilience of the Internet to random breakdowns, Phys. Rev. Lett. 85 (21) (2000) 4626–4628.
[12] R. Cohen, K. Erez, D. ben-Avraham, S. Havlin, Breakdown of the internet under intentional attack, Phys. Rev. Lett. 86 (16) (2001) 3682–3685.
[13] L.K. Gallos, R. Cohen, P. Argyrakis, A. Bunde, S. Havlin, Stability and topology of scale-free networks under attack and defense strategies, Phys. Rev. Lett. 94 (18) (2005) 188701.
[14] A. Vazquez, Y. Moreno, Resilience to damage of graphs with degree correlations, Phys. Rev. E 67 (1) (2003) 015101.
[15] S. Sun, Z.X. Liu, Z.Q. Chen, Z.Z. Yuan, Error and attack tolerance of evolving networks with local preferential attachment, Physica A 373 (2007) 851–860.
[16] B. Shargel, H. Sayama, I.R. Epstein, Y. Bar-Yam, Optimization of robustness and connectivity in complex networks, Phys. Rev. Lett. 90 (6) (2003) 068701.
[17] G. Paul, T. Tanizawa, S. Havlin, H.E. Stanley, Optimization of robustness of complex networks, Eur. Phys. J. B 38 (2) (2004) 187–191.
[18] T. Tanizawa, G. Paul, R. Cohen, S. Havlin, H.E. Stanley, Optimization of network robustness to waves of targeted and random attacks, Phys. Rev. E 71 (4) (2005) 047101.
[19] R.V. Solé, S. Valverde, Information theory of complex networks: On evolution and architectural constraints, Complex Netw. 650 (2004) 189–207.
[20] B. Wang, H.W. Tang, C.H. Guo, Z.L. Xiu, Entropy optimization of scale-free networks' robustness to random failures, Physica A 363 (2) (2006) 591–596.
[21] Y.H. Xiao, W.T. Wu, H. Wang, Symmetry-based structure entropy of complex networks, Phys. A: Stat. Mech. Appl. 387 (11) (2008) 2611–2619.
[22] J. Wu, Y.J. Tan, H.Z. Deng, D.Z. Zhu, Normalized entropy of rank distribution: a novel measure of heterogeneity of complex networks, Chin. Phys. 16 (6) (2007) 1576–1578.
[23] Y. Zhuo, Y.F. Peng, C. Liu, Y.K. Liu, K.P. Long, Improving the attack tolerance scale-free networks by adding and hiding edges, Phys. Scr. 83 (2011) 025801.
[24] S. Xiao, G. Xiao, On intentional attacks and protections in complex communication networks, in: Proceedings of the 2006 IEEE GLOBECOM'06, Nov. 2006, pp. 1–5.
[25] Z. Wang, M. Jusup, W. Wang R, et al., Onymity promotes cooperation in social dilemma experiments., Sci. Adv. 3 (3) (2017) e1601444.
[26] X. Li, M. Jusup, et al., Punishment diminishes the benefits of network reciprocity in social dilemma experiments, Proc. Natl. Acad. Sci. U.S.A. 1 (115) (2018) 30–35.
[27] W. Zhen, J. Marko, S. Lei, et al., Exploiting a cognitive bias promotes cooperation in social dilemma experiments, Nat. Commun. 9 (1) (2018) 2954.
[28] C. Shen, C. Chu, L. Shi, et al., Coevolutionary resolution of the public goods dilemma in interdependent structured populations, EPL (Europhys. Lett.) 124 (4) (2018).
[29] L. Shi, C. Shen, Y. Geng, et al., Winner-weaken-loser-strengthen rule leads to optimally cooperative interdependent networks, Nonlinear Dyn. 96 (1) (2019) 49–56.
[30] J. Wu, M. Barahona, Y.J. Tan, et al., Natural connectivity of complex networks, Chin. Phys. Lett. 27 (7) (2010) 078902.
[31] H.J. Herrmann, C.M. Schneider, A.A. Moreira, et al., Onion-like network topology enhances robustness against malicious attacks, J. Stat. Mech. Theory Exp. 2011 (01) (2011) P01027.
[32] C. Salavati, A. Abdollahpouri, Z. Manbari, Ranking nodes in complex networks based on local structure and improving closeness centrality, Neurocomputing 7 (336) (2019) 36–45.
[33] L. Benguigui, I. Porat, Relationships between centrality measures of networks with diameter 2, Phys. A-Stat. Mech. Appl. 1 (505) (2018) 243–251.
[34] F. Yang, X. Li, Y. Xu, Ranking the spreading influence of nodes in complex networks: an extended weighted degree centrality based on a remaining minimum degree decomposition, Phys. Lett. A 31 (382) (2018) 2361–2371.