IDENTIFICATION OF KEY NODES IN EQUIPMENT SYSTEM NETWORK BASED ON FUNCTION CHAIN

Cheng Huang, Yong Gang Li and Ying Wang

School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chong Qing, China

ABSTRACT

With the rapid development of modern military technology, the combat mode has been upgraded from traditional platform combat to system-level confrontation. In traditional combat network, node function is single and which is no proper assignment of tasks. The equipment system network studied in this paper contains many different functional nodes, which constitute a huge heterogeneous complex network. Most of the key node identification methods are analyzed from the network topology structure, such as degree, betweenness, K-shell, PageRank, etc. However, with the change of network topology, the identification effect of these methods will be biased. In this paper, we construct a nodal attack sequence, Consider the change of the number of effective OODA chains in the equipment system network after the nodes in the sequence are attacked. And combined with the improved Gray Wolf optimization algorithm, this paper proposes a key node evaluation model of equipment system network based on function chain —— IABFI. Experimental results show that the proposed method is more effective, accurate, and applicable to different network topologies than other key node identification methods.

KEYWORDS

Equipment system network, node sequence attack, effective OODA chain, improved Grey Wolf optimization algorithm.

1. INTRODUCTION

Modern military technology is evolving rapidly, and the mode of operation has shifted to system-level combat versus a single weapon platform [1, 2]. It is not a single soldier or a stand-alone operation as we have in mind. It emphasizes the communication between the parts and the division of labor. The equipment system network is a complex heterogeneous network, which is a higher-level whole body composed of various weapons and equipment systems that are connected and interact with each other in terms of function. The network contains a variety of nodes with different functions [3]. In this complex network of equipment system, the importance of different nodes is very different. Once a very important node is attacked and fails, the whole network of equipment system will be greatly affected [4]. Therefore, in this era of rapid development of military technology. Accurately and quickly find out the key nodes in the network, protect our important nodes, hit the enemy's key nodes, So asto win the battle, has epoch-making significance.

Project supported by the National Defense PreResearch Quick Support Foundation of China (no.80911010 302)

David C. Wyld et al. (Eds): NATP, ACSTY, CCCIOT, MLSC, ITCSS - 2022
pp. 01-16, 2022. CS & IT - CSCP 2022 DOI: 10.5121/csit.2022.120101

At present, key node identification in complex networks is mostly based on isomorphic network model, that is, in current key node identification, only the same type of nodes and edges exist in the studied network. These studies do not take into account the heterogeneity of the equipment system network, which can't adapt to the large-scale military system confrontation, so the algorithm proposed by them can't be well applied to the combat research of heterogeneous network. At present, the identification of key nodes mainly considers the network topology structure, such as degree centrality, betweenness centrality, K-shell, PageRank and so on [5]. Or consider the combination of weights, comprehensively consider the weights of evaluation indicators from both subjective and objective dimensions, and then multiply the indicators by the corresponding weights, sum up, to get the sequence of important nodes [6]. These traditional indicators and methods can accurately identify key nodes in some specific scenarios, but the structure and scale of the network will not remain unchanged [7, 8]. Nowadays, with the increasingly large structure and scale of equipment system network, these traditional indexes and methods are obviously unable to meet the needs of large-scale military operations.

In this paper, considering the complex combat tasks of the equipment system, according to the requirements of combat tasks, the network nodes of the equipment system are divided into sensor node S, command node D and strike node I [9]. S nodes, D nodes and I nodes are combined to form a complete chain of reconnaissance, decision making and strike to complete combat missions. According to the above, this paper proposes a key node identification and evaluation model of equipment system network based on function chain——IABFI. By combining the function chain with the improved grey Wolf optimization algorithm, the overall identification method can achieve a more accurate identification effect on the equipment system network of different sizes and structure.

2. ROBUSTNESS MEASUREMENT OF EQUIPMENT SYSTEM NETWORK BASED ON FUNCTION CHAIN

Equipment system network robustness refers to the remaining operational capability of the entire equipment system network after some nodes or edges are attacked.Due to the large difference between the topological structure of equipment system network and the traditional complex network, the traditional methods to measure the robustness of homogeneous network, such as the maximum connected component and network efficiency, are not suitable for heterogeneous equipment system network. In this paper, effective OODA chain is introduced to measure the robustness of equipment system network. The operational effectiveness of modern military operations is no longer a solitary struggle. Considering the performance index of a single machine, it is more important to consider the information interaction between each equipment entity. The communication of control and command information among individual machines has an important influence on the overall confrontation of the system. In the equipment system network, the equipment entity is abstracted as node, and the information transfer is abstracted as edge. Before introducing OODA chains, let's first introduce OODA rings, as shown in figure 1.

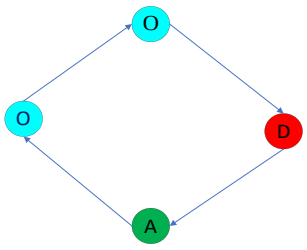

Figure 1. OODA ring model

A complete military operation has four steps: Observe (O) $\rightarrow$ Orient (O) $\rightarrow$Decide (D) $\rightarrow$Act (A). In the network of equipment systems, The OODA ring can be abstracted as an SDI chain model.

As shown in figure 2, in the function chain, combat information starts from node S, passes through node D, and finally reaches node I, which is directional.

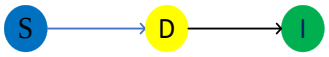

Figure 2. SDI chain model

However, there may be many $S \rightarrow S$ and $D \rightarrow D$ in the SDI chain, which leads to the concept of a generalized SDI chain, as shown in figure 3.

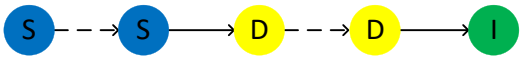

Figure 3. Generalized SDI chain model

For the equipment system network, we put forward the concept of effective OODA chain. The effective OODA chain can be understood as the same function chain, even if the connection mode is different, as long as the node set involved in the same function chain is consistent. as shown in figure 4, in the equipment architecture network model, $S_4 \rightarrow S_5 \rightarrow D_4 \rightarrow I_5$ and $S_5 \rightarrow S_4 \rightarrow D_4 \rightarrow I_5$ can be viewed as the same chain of functions. A valid OODA chain is calculated as shown in formula (1).

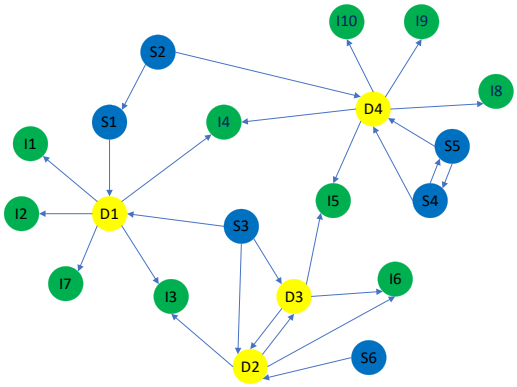

Figure 4. Network model of equipment system based on function chain

$$V_{\text{num}} = \prod(\sum_{i}^{n} D^{i}_{in\_degree\_S} \times D^{i}_{adjoin\_in\_S})(\sum_{i}^{n} D^{i}_{out\_degree\_I} \times D^{i}_{adjoin\_out\_I}) \quad (1)$$

In formula (1), V_{num} represents the number of valid OODA chains, $D^{i}_{in\_degree\_S}$ is the number of S nodes connected to the $i-th$ D node, $D^{i}_{adjoin\_in\_S}$ is the number of adjacent S nodes of adjacent S nodes connected to the $i-th$ D node.

Network performance is represented by the change in the number of effective OODA chains after i nodes are removed from the equipment system network. Obviously, a simple $S \rightarrow D$ chain, such a link does not attack node i, there is no way to inflict a blow on the enemy. Or $D \rightarrow I$ chain, no reconnaissance node S, clueless blind attack, such a combat link is not good. Therefore, in an equipment system network, the greater the number of OODA chains, the higher the network performance and the stronger the network robustness. Assuming that network G has n nodes with labels ranging from 1 to N, a node sequence $k = \{k_1, k_2, k_3, k_4, \cdots, k_n\}$ can be specified. Attack and remove nodes in sequence according to the node sequence. With the removal of nodes, the cumulative robustness of the equipment system network under sequence K is defined as:

$$CR(G,K) = \sum_{i=1}^{n} V_{num}(i) \qquad (2)$$

$V_{num}(i)$ represents the number of valid OODA chains remaining in the network after the i-th node in the equipment system network G is attacked. With different node sequences K, the cumulative robustness CR of the network is different. The smaller CR is, the more destructive the removal of nodes according to the corresponding node sequence will be to the network of the equipment system, and the sequence of nodes arranged in the node sequence will be more accurate [10].

3. IDENTIFICATION OF KEY NODES BASED ON IMPROVED GRAY WOLF OPTIMIZATION ALGORITHM

3.1. Basic Gray Wolf Optimization Algorithm

For the equipment system network G, we rank nodes according to their importance degree from high to low, and the network robustness obtained in this order will also reach the minimum. If we find a corresponding equipment system network G, and the sequence robustness CR reaches the minimum, then this sequence is the best sequence we require. Based on the above ideas, we can get out of the limitation of analyzing node importance from network topology. Whether it is degree centrality, betweenness centrality or K-shell sorting algorithm, the accuracy of these sorting algorithms varies greatly in different network topologies. The attack sequence of nodes is constructed based on the improved Gray Wolf optimization algorithm, and the identification of key nodes is transformed into a function optimization problem, which has high accuracy and is suitable for various network structures. The goal of this paper is to construct a node sequence K that minimizes the cumulative robustness CR(G,K) of the equipment system network after nodes are attacked and invalid. The construction function is shown in formula (3):

$$\begin{cases} \min & \text{CR(G,K)} \\ s.t. & \text{K} \in Set\_k \end{cases} \qquad (3)$$

The above Set_k is a set, which contains the attack sequences of all nodes against the target equipment system network G.

The node size of the equipment system network is very large, and it is normal to have thousands of nodes. And when the studied equipment system network G contains n nodes, the number of elements in Set_k is $n!$. Faced with such a huge solution space scale problem, we consider using intelligent search algorithm. In view of the excellent convergence stability and strong global search ability of the Gray wolf optimization algorithm, this paper adopts the Gray wolf optimization algorithm to realize the sequence optimization and identify the optimized node sequence[11]. Gray wolf optimization algorithm is a heuristic intelligent algorithm proposed by Mirjalili et al in 2014, it is a relatively new optimization technique that simulates the leadership hierarchy of pack hunting in a grey wolf pack, which takes on a golden tower shape[12], as shown in figure 5.

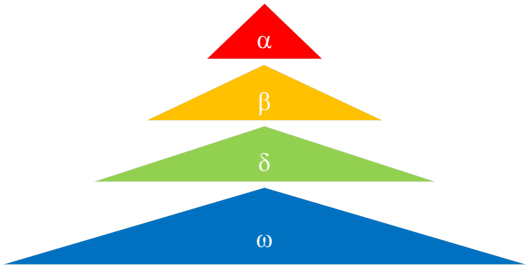

Figure 5. Leadership hierarchy of Gray Wolf pack [13]

As we all know, the Gray wolf is a social carnivore. The Gray wolf family is divided into four classes : α、 β、 δ、 ω . As can be seen from fig.5, wolf α is the top wolf in the Gray wolf world, serving as the leader, followed by the deputy leader, wolf β . wolf ω is the bottom wolf. wolf δ obeys the rule of wolf α and wolf β , but it can manage wolf ω [14].

Search process: when Gray Wolf is searching for prey, a very important judgment standard that prompts Gray Wolf to take hunt is according to the distance between oneself and prey. Let's say we're in the t-th iteration of the search, $X(t)$ is the position of the Gray Wolf, $X_p(t)$ is the position of the prey, then the distance between the Gray Wolf and the prey is shown in formula (4):

$$\begin{cases} D = \left| C \bullet X_p(t) - X(t) \right| \\ C = 2r_2 \\ r_2 = rand(0,1) \end{cases} \quad (4)$$

Encircle process: In the process of encircle prey, Gray wolf establishes the relationship model between Gray wolf and prey according to the distance between them, so as to realize the process of encircle prey. The relation model is shown in formula (5):

$$\begin{cases} X_i^d(t+1) = X_p^d(t) - A_i^d \bullet D_i^d \\ D_i^d = \left| C_i^d \bullet X_p^d(t) - X_i^d(t) \right| \\ A_i^d = 2ar_1 - a \\ C_i^d = 2ar_2 \\ a = 2 - t/t_{\max} \\ r_1, r_2 = rand(0,1) \end{cases} \quad (5)$$

In Formula 5, $A_i^d \bullet D_i^d$ represents the envelop step size in the process of envelop prey, and the maximum number of iterations is represented by $t_{\max}$ in the formula, t is the current number of iterations. For $a = 2 - t / t_{\max}$, we can see that the parameter, a, decreases linearly from 2 to 0. The random initialization of A_i^d and C_i^d ensures that the Gray Wolf will not easily fall into the local optimal position in the process of the search, and can easily reach the global optimal position.

Position update (attack): We can accurately and quickly judge the position of target prey through the position information updated by wolf α, wolf β and wolf δ.

$$\begin{cases} X_1 = X_\alpha - A_1 \bullet D_\alpha \\ X_2 = X_\beta - A_2 \bullet D_\beta \\ X_3 = X_\delta - A_3 \bullet D_\delta \\ X = (X_1 + X_2 + X_3)/3 \end{cases} \quad (6)$$

In formula 6, the positions of wolf α, wolf β and wolf δ are represented by X_1, X_2 and X_3 respectively. A_1, A_2 and A_3 are three random numbers. $A_1 \bullet D_\alpha$、 $A_2 \bullet D_\beta$ and $A_3 \bullet D_\delta$ represent the encircling steps of wolf α, wolf β and wolf δ, X is the final position, where the wolf attacked its prey.

The Gray wolf has strong global ability through the variation of speed, the change of search radius at any time, the update of position and other strategies, and it is easier for the Gray wolf to get the optimal solution and suboptimal solution in the global scope [15].

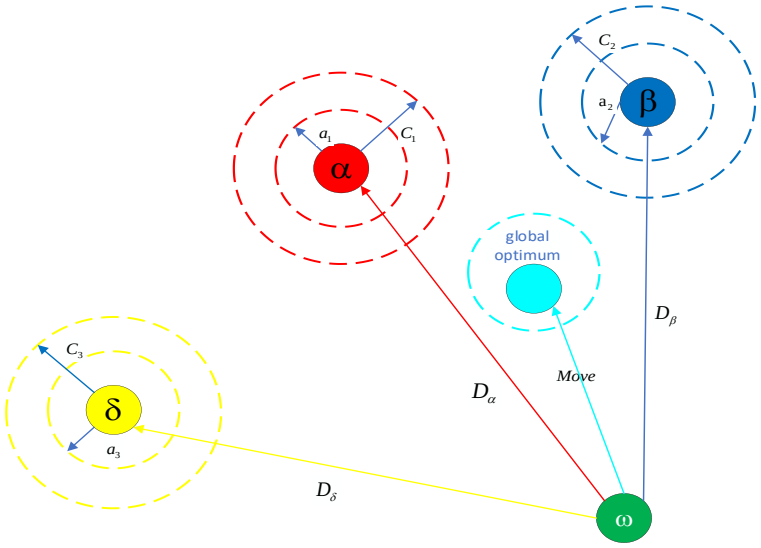

Figure 6. Position update of Gray Wolf in Gray Wolf optimization algorithm [15]

3.2. Improvement of Gray Wolf Optimization Algorithm

The grey wolf optimization algorithm has a fast convergence rate in the initial stage, and the wolves' position changes greatly, so it has strong global search performance. However, as the number of iterations increases in the later period, and changes in position become less volatile, which will easily lead to the algorithm falling into local optimal. To make up for this shortcoming, let's make some improvements to the Gray Wolf algorithm.

(1) Construction of the objective function: The robustness of the equipment system network based on function chain is studied in this paper. In the equipment system network, nodes are attacked in sequence according to the sequence of nodes, and the cumulative robustness of the equipment system network is calculated as the nodes are removed.

To solve the problem of the cumulative robustness of the equipment system network under the node sequence K, we introduce the Gray Wolf algorithm: The population size of Gray Wolf is N, and the number of nodes in the equipment system is D. In the D-dimensional node search space, the position of the i-thGray wolf is X (that is, the node sequence of the equipment system network), As defined in formula (7):

$$X_i = (X_i^1, X_i^2, X_i^3, \cdots X_i^{D-1}, X_i^D) \tag{7}$$

According to the Gray wolf algorithm, when N Gray wolves search for prey in the D-dimensional space, space domain P can be defined as a matrix, as follows:

$$P=\begin{bmatrix} X_1^1 & X_1^2 & \cdots & X_1^j & \cdots & X_1^{D-1} & X_1^D \\ X_2^1 & X_2^2 & \cdots & X_2^j & \cdots & X_2^{D-1} & X_2^D \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ X_i^1 & X_i^2 & \cdots & X_i^j & \cdots & X_i^{D-1} & X_i^D \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ X_N^1 & X_N^2 & \cdots & X_N^j & \cdots & X_N^{D-1} & X_N^D \end{bmatrix} \quad (8)$$

In formula (8), $X_i^j(i \le N, j \le D)$ represents the position of the i-th Gray Wolf in j-th dimension in the spatial domain P. Each line represents a sequence of positions of a Gray Wolf in the search space, that is, a sequence of nodes in the equipment system network. What is required is to find a sequence among these node sequences that minimizes the cumulative robust CR(G,K) of the equipment system network, The value of the objective function f is calculated by $f = \min \ \mathrm{CR(G,K)}$.

To sum up, when the number of nodes to be solved is D, what we need to take is to find an optimal position K of Gray Wolf population, so that the objective function value f is the minimum.

$$\begin{cases} f = \min \quad \mathrm{CR(G,K)} \\ s.t. \quad \mathrm{K} \in Set\_k \end{cases} \quad (9)$$

G is the equipment system network topology. K is a Gray Wolf position.

(2) Construction of initial solution: in the process of Gray wolf algorithm optimization, a good initial solution is particularly important for iterative optimization, which helps to reduce the algorithm complexity and optimization time. For finding the key nodes in the network of the equipment system, the relative quality of the initial solution generated in a random way is very low. The damage of attacking core nodes is much greater than that of attacking marginal nodes, which can result in the sharp reduction of effective OODA chain in the equipment system network.

According to the above idea, the weak centrality $VR(i)$ of node $i(1 \le i \le n)$ is defined as:

$$VR(i) = V_{num} - V_{num}(i) \quad (10)$$

V_{num} represents the number of effective OODA chains in the initial equipment system network. $V_{num}(i)$ indicates the number of remaining valid OODA chains in the network after the i-th node in the installation system network G is attacked. According to formula 10, the larger $VR(i)$ is, the more important node i is. According to the calculation, we take the node i with the highest $VR(i)$ value as the first node in the sequence, then the values are sorted from large to small until a complete sequence of node attacks is constructed.

(3) 2-opt optimization algorithm:2-opt optimization is also known as pairwise swapping, which is a local search algorithm[16]. When we update the position of the Gray wolf, we use this method

of exchanging the two datas, which effectively avoids the blind disorder when the Gray wolf changes the position.

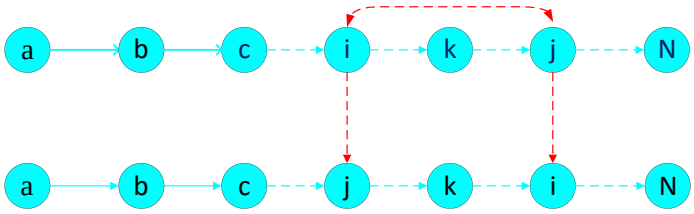

Figure 7. 2—opt schematic diagram[14]

As shown in figure 7, assuming that the second node sequence makes the value of the objective function smaller, the system network node i and j are exchanged, and the position number of the Gray wolf is updated.

The node solution vector of the equipment system network can be expressed as:

$$X_i = (X_i^1, X_i^2, \cdots, X_i^{D-1}, X_i^D) \quad (11)$$

In formula 11, $i(i = 1,2,3 \cdots N)$ is the i-th Gray Wolf in the Gray Wolf population, D is the serial number of the network node of the equipment system traversed by the Gray Wolf. According to the size of the distance between the solution vectors, we choose the two nodes whose distance between the solution vectors is shorter and then exchange the two nodes.

The core of 2-0PT optimization algorithm: The cumulative robustness of the equipment system network after switching nodes is calculated. If the value becomes smaller, it indicates that it is indeed optimized, and we retain the current solution vector as the optimal solution of this Gray Wolf; otherwise, the solution vector remains unchanged. Continue to make the above judgment for the next line of Gray wolves until all the solution vectors of Gray wolves have been optimized, solution vectors of grey Wolf in all rows are traversed, and the solution with the smallest objective function value and its solution vector are retained. At this point, we have completed a loop.

(4) Elite selection system: In the process of searching solution vector, Gray Wolf algorithm is always accompanied with random and blindness. In order to deal with this problem, we adopt the elite selection system to improve the node sorting path. In the large-scale iterative optimization process, we retain some better node sorting, which is called elite. We retain these elites as the starting sequence of nodes for the next cycle, which can greatly improve the speed of calculation and reduce the complexity of the algorithm to a large extent.

3.3. Key node identification method—IABFI

With the above improved strategy, the critical node identification process with cumulative robust CR as the objective function is shown in figure 8.

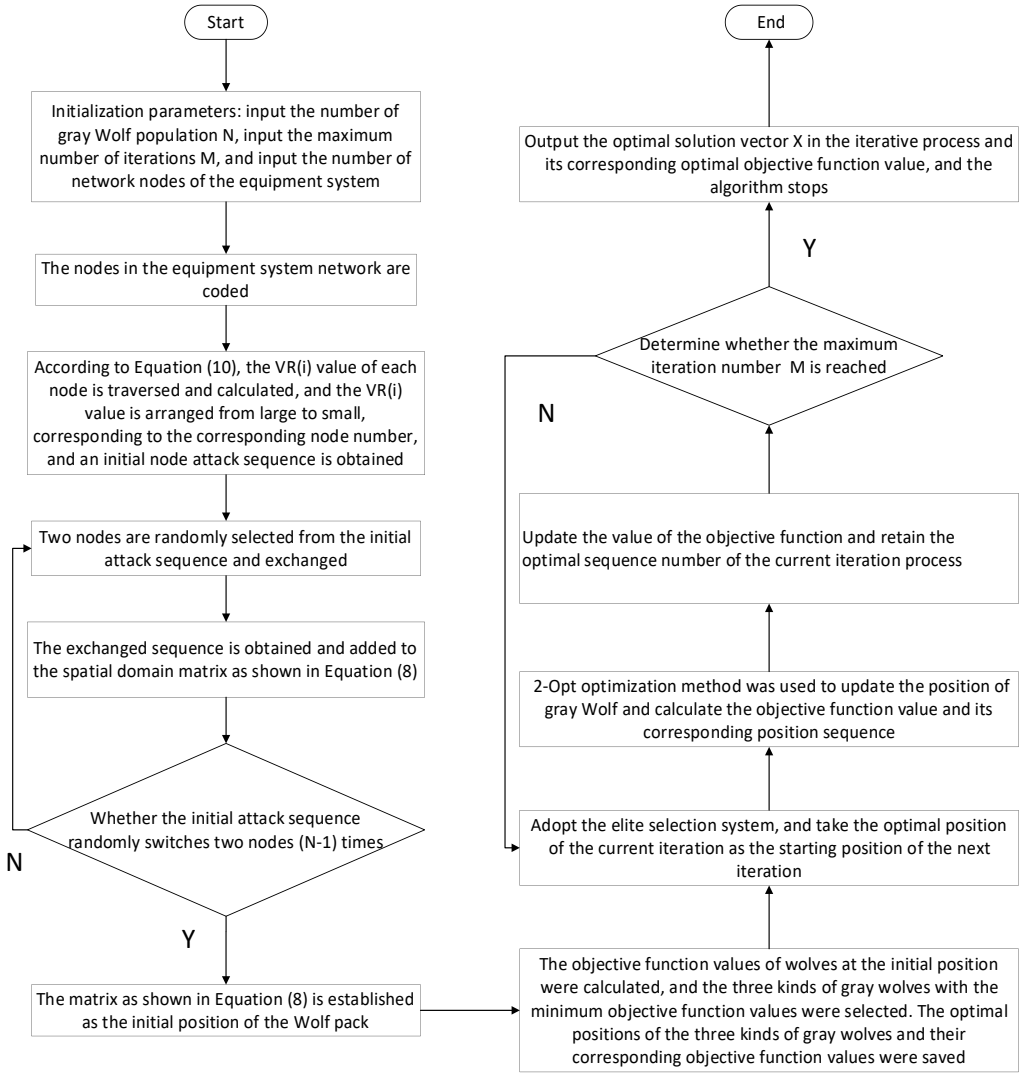

Figure 8. IABFI—key node identification flowchart

4. EXPERIMENTAL SIMULATION AND ANALYSIS

In order to verify the superiority of the proposed IABFI - node identification algorithm in searching key nodes in the equipment system network. In this section, network models of equipment system based on random networks (ER), small world networks (WS) and scale-free networks (BA) are established respectively, They correspond to Figures 9, 10 and 11 below, and verified under different network scales. The key node identification algorithm proposed in this paper is compared with the traditional algorithms of betweenness centrality, degree centrality, improved K-shell algorithm, PageRank algorithm, eigenvector centrality, closeness centrality, etc. According to the order of nodes arranged by each algorithm, the corresponding nodes are attacked in turn, and the simulation is carried out in the above three devices system network.

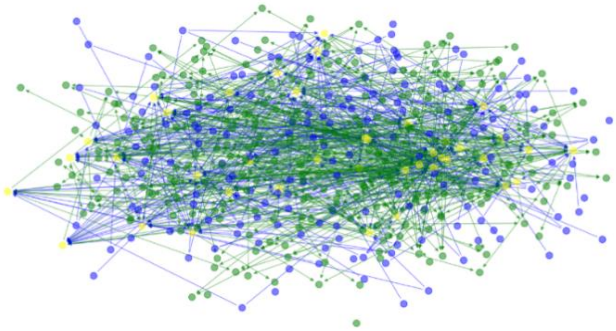

Figure 9. Network model of equipment system based on random network

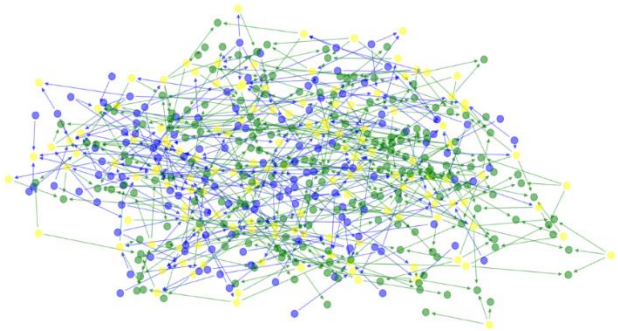

Figure 10. Network model of equipment system based on small world network

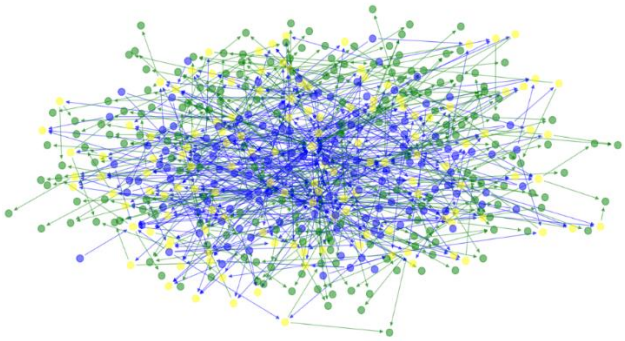

Figure 11. Network model of equipment system based on scale-free network

Combined with corresponding military applications, the scale of the above three equipment system network models is 450 nodes, in which S node is blue, D node is yellow, and I node is green.

After the importance of nodes is sorted according to the corresponding algorithm index, the nodes in the equipment system network are attacked in sequence according to the order of node importance. As nodes are attacked, they become ineffective, and the number of effective OODA chains in the equipment system network decreases, which is accompanied by the decrease of the operational performance of the equipment system network.

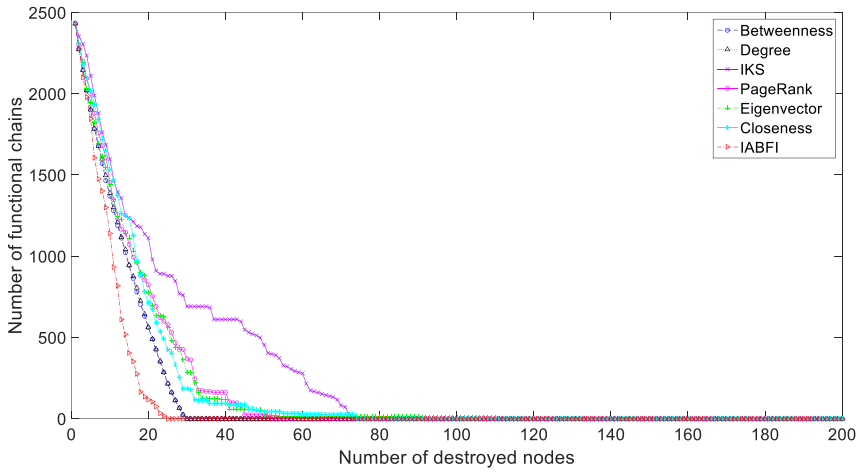

Figure 12. Network performance variation of equipment system based on random network (200 nodes)

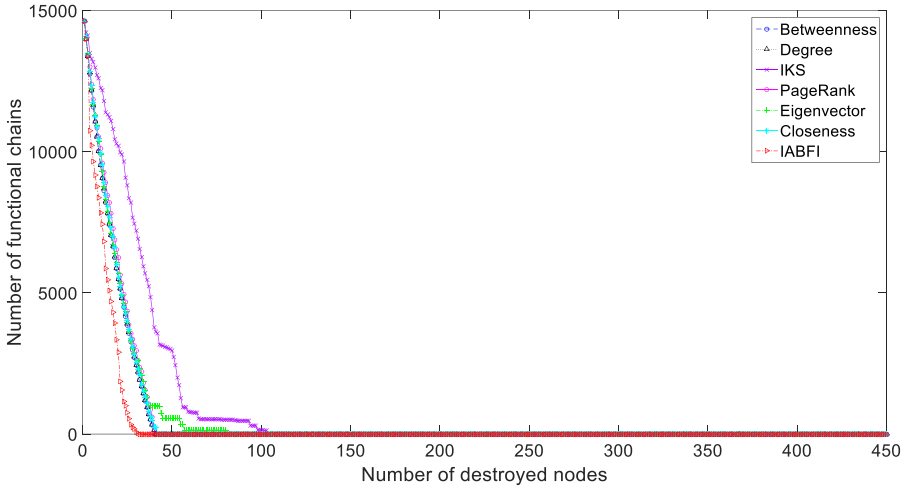

Figure 13. Network performance variation of equipment system based on random network (450 nodes)

Figure 12 and Figure 13 show the network model of equipment system based on random network with node size of 200 and 450 respectively. In these two networks, the nodes are sorted according to the above indexes, and the nodes are hit in sequence according to the sorted sequence. The effective OODA chain is reduced in the equipment system network of the above two scales. In fig.12, there are 2432 original OODA chains at the initial time. A node sequence is obtained based on IABFI algorithm. After the first 24 nodes in the sequence are attacked, there is no function chain in the whole network. In other sorting algorithms, the effect is relatively good is the intermediate centrality and degree centrality. These two algorithms sort the sequence, the number of OODA chains in the entire equipment system network is zero until the first 29 nodes in the sequence are attacked. Others such as PageRank algorithm, feature vector centrality, proximity, improved K-shell algorithm, the sequence obtained by the arrangement of these algorithms. According to sequence, after the first 51, 110, 73 and 72 nodes are attacked, the function chain completely disappears. In addition, it can be seen from the figure above that, compared with other algorithms, the function chain in the equipment system network declines particularly fast after the nodes are attacked according to the sequence sorted by IABFI algorithm, the number of function chains decreases rapidly at the beginning and then slows down,

which fully demonstrates the effectiveness of the algorithm for node sorting. According to the sequence sorted based on the IABFI algorithm, the nodes are attacked sequentially. The nodes initially attacked are generally the hub nodes connected with a large number of OODA chains. After being attacked, the number of OODA chains in the equipment system network is greatly reduced. As shown in Figure 13, the original number of OODA chains is 14,621. After the attack, the downward trend is basically consistent with the model diagram of 200 nodes. In fig.13, the number of function chains in the equipment system network is large, Under the ranking attack of algorithms such as closeness centrality, eigenvector centrality and PageRank algorithm, the difference between algorithms in fig. 13 is less obvious than that in fig. 12. However, it is still clear that compared with other traditional algorithms, the effect of IABFI algorithm is still more obvious.

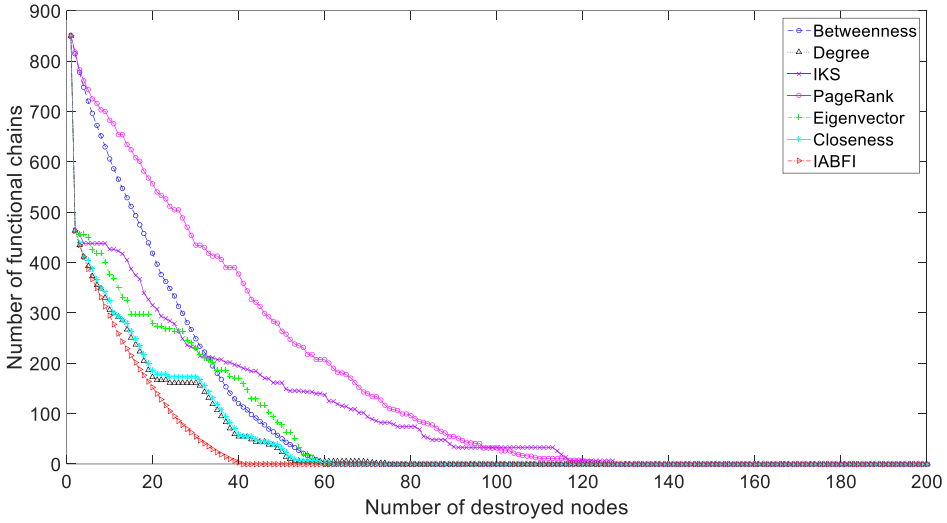

Figure 14. Network performance variation of equipment system based on small world network(200 nodes)

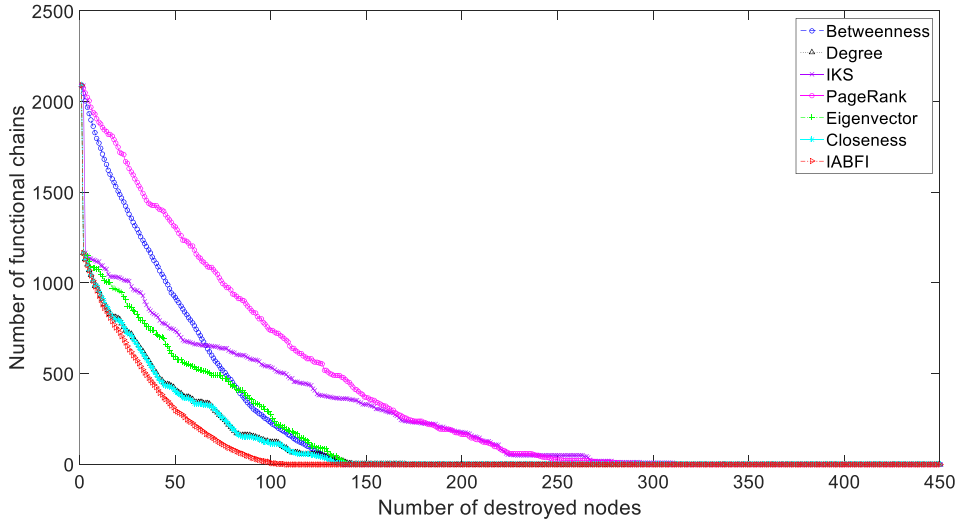

Figure 15. Network performance variation of equipment system based on small world network (450 nodes)

In the above small world network based on equipment system model, there is an important node at the beginning. Betweenness centrality and PageRank algorithm did not find this node in time. As a result, its recognition effect is not very good compared with that in the random network of equipment system network model. Compared with the random network model, the relative error of the PageRank algorithm is more huge. In Figure 14, after the first 125 nodes in the equipment system network are attacked, its function chain is 0, and its cumulative robustness is as high as 32,244, the cumulative robustness of IABFI algorithm in the same period is 7467. It can still be clearly seen from the above two figures that compared with other algorithms, IABFI algorithm still has the most obvious effect. After nodes in the equipment system network are attacked, the decline trend is the most dramatic. In Figure 14, sorted by IABFI algorithm, after attacking the 40 nodes in the sequence, the function chain in the equipment system network is 0, and the effect is the best. In Figure 15, the effect trend is similar to that in Figure 14. According to the simulation diagram of attack effect of WS network nodes of different scales, it can be seen that IABFI algorithm is applicable to the equipment system network of different scales mentioned above.

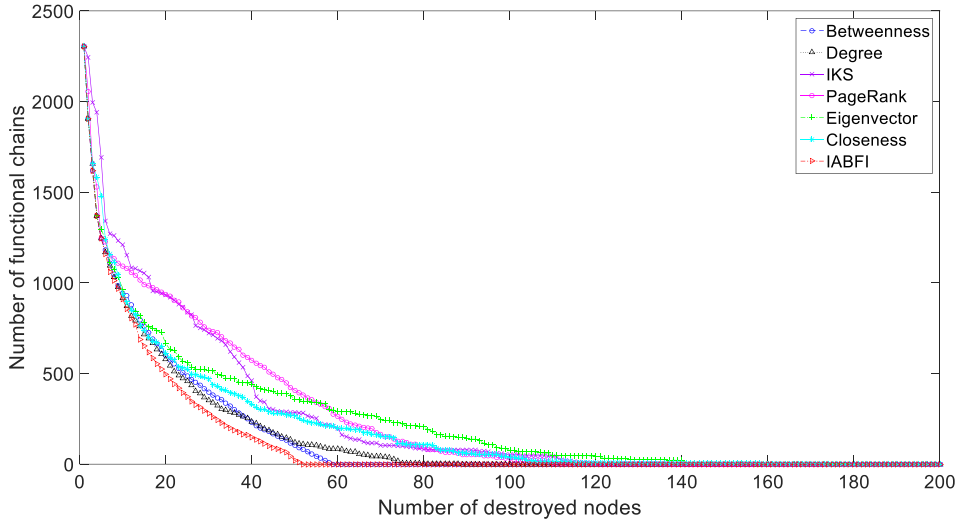

Figure 16. Network performance variation of equipment system based on scale-free network (200 nodes)

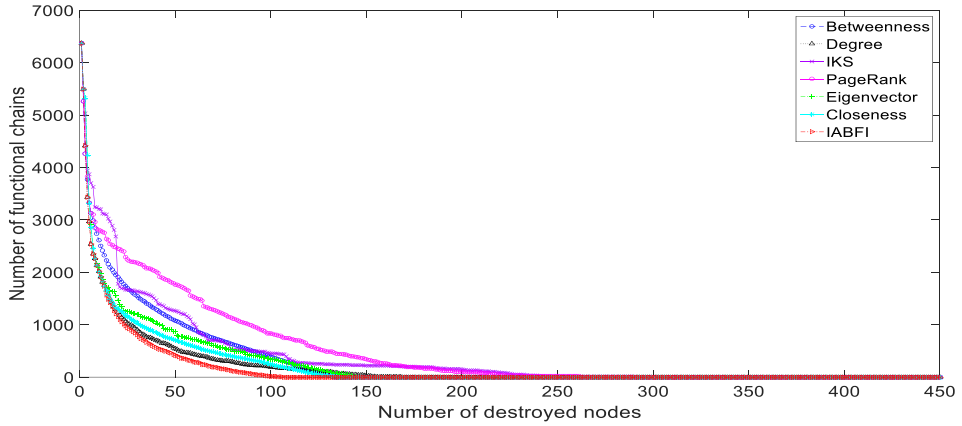

Figure 17. Network performance variation of equipment system based on scale-free network (450 nodes)

We conduct further simulation under scale-free network. As shown in FIG. 16 and 17, the optimization effect of IABFI algorithm is as efficient and accurate as always in scale-free network. Compared with the traditional algorithm which is affected by the network topology structure, the performance of the algorithm differs greatly under different network models. It can be seen that the performance of IABFI algorithm has been stable, and compared with the traditional algorithm, the performance is also the most superior. As can be seen from the figure above, according to the IABFI algorithm, after the nodes in the sequence are hit, the number of OODA chains in the equipment system network still declines the fastest.

According to the above six simulation graphs, the variation trend of the number of function chains in the equipment system network after the nodes in the equipment system network are attacked is compared under different topologies and node sizes. Compared with other algorithms, IABFI algorithm can identify key nodes accurately and quickly, and it is suitable for different network models, unlike the traditional node identification algorithm in different equipment system network model performance difference, it shows that the IABFI algorithm is effective and stable.

5. CONCLUSIONS

The application of optimization algorithm to node optimization has also appeared in previous researches on isomorphic networks. Single point optimization based on tabu search algorithm or discrete firefly algorithm, complex network robustness measure considering network efficiency. They have their own advantages and disadvantages under different measurement indexes. In this paper, effective OODA chain is considered, and the improved Gray Wolf algorithm has more prominent advantages in convergence speed and global search than other algorithms. According to the analysis of the change of the number of effective OODA chains after the network nodes of the equipment system are attacked in sequence with the sequence K, it is shown that compared with other traditional node sorting algorithms, IABFI can be applied to network models with different network topologies and different node sizes, and its performance is more stable. It can find the key nodes in the network most quickly. The IABFI algorithm can be used to quickly find out the key nodes in the equipment system network, and in the military action against the enemy, it can find out the key nodes, take decapitation action, and destroy the enemy's military operation network in the shortest time. At the same time, IABFI algorithm can also be used to find out the important key nodes in our equipment system network, backup and take priority protection strategies for the important nodes. It can ensure that we can maintain the original function of our equipment system network and win the battle in the face of external attack in the fierce military confrontation. However, in the process of our study, we found that it is often difficult to simulate when drawing large-scale node graph. When the node scale is large, the speed of simulation results is also slow. In the following research process, we will do targeted research on this issue.

ACKNOWLEDGEMENTS

Project supported by the National Defense PreResearch Quick Support Foundation of China (no.80911010 302)

REFERENCES

[1] Z.Ni, (2004) “Modeling and simulation of weapon system confrontation”, Military Operations Research and Systems Engineering, Vol. 18, No. 1, pp2-6.

[2] K. Li, W. Wu, (2016) “Research Status of Weapon Equipment System-of-Systems Based on Complex Network”, Journal of Academy of Armored Force Engineering, Vol. 30, No. 4, pp7-13.

[3] J. Wang, M. Wang. & W. Ding, (2016) “A Value-Focused Decision Making Framework for System of Systems Architecture”, Computer & Digital Engineering, Vol. 44, No. 10, pp1948-1951+1962.
[4] R. Li, H. Zhang. & Y. Yin, (2011) “The ideal understanding of several basic problems of weapon equipment architecture optimization”, Military Operations Research and Systems Engineering, Vol. 25, No. 2, pp5-10.
[5] Deng Y, Wu J & Tan YJ, (2016) “Optimal attack strategy of complex networks based on tabusearch”, Physica A Statistical Mechanics, Vol. 442, No. 1, pp74-81.
[6] X. Liu, G. Xu & P. Yang, (2019) “Node importance evaluating of network based on combination weighting VIKOR method”, Application Research of Computers, Vol. 36, No. 8, pp2368-2371+2377.
[7] T. Wang, W. Dai & P. Jiao, (2016) “Identifying influential nodes in dynamic social networks based on degree-corrected stochastic block model”, International Journal of Modern Physics B, Vol. 30, No. 16.
[8] Z. Shao, S. Liu &Y. Zhao, (2019) “Identifying influential nodes in complex networks based on neighbours and edges”, Peer-to-Peer Networking and Applications, Vol. 12, No. 6, pp1528-1537.
[9] H. Li, L. Zhou & W. Xin, (2017) “Optimization of networked Combat Equipment Architecture based on optimal tree”, Military Operations Research and Systems Engineering, Vol. 31, No. 4, pp47-53.
[10] X. Feng, C.Hu. & C. Xu, (2019) “Key node recognition method based on optimal network efficiency”, Computer Engineering And Design, Vol. 40, No. 2, pp328-335.
[11] MIRJALILI S, MIRJALILI S M& LEWIS A, (2014) “Grey wolf optimizer”, Advances in Engineering Software, Vol. 69, No. 7, pp46-61.
[12] S. Gao, L. Meng, (2019) “Greedy randomized adaptive grey wolf optimization algorithm for solving TSP difficulty”, Modern Electronics Technique, Vol. 42, No. 14, pp46-50+54.
[13] X. Zhang, Y. Zhang & Z. MING, (2021) “Improved dynamic grey wolf optimizer”, Frontiers of Information Technology & Electronic Engineering, Vol. 22, No. 6, pp877-891.
[14] R.XU, M. Cao. &M. Huang, (2018) “Research on TSP-like problem based on improved Gray Wolf optimization algorithm -- taking tourism as an example”, Geography and Geo-Information Science, Vol. 34, No. 2, pp14-21.
[15] SAREMI S, MIRJALILI S Z& MIRJALILI S M, (2015) “Evolutionary population dynamics and grey wolf optimizer”, Neural Computing and Applications, Vol. 26, No. 5, pp1257-1263.
[16] CROES G A, (1958) “A method for solving traveling-salesman problems”, Operations Research, Vol. 6, No. 6, pp791-812.

AUTHORS

Cheng Huang graduated from The Department of Electronics and Information Engineering of Chifeng University in 2019 with a bachelor's degree. He is currently pursuing a master's degree in school of communication and information engineering at Chongqing University of Posts and Telecommunications in Chongqing, China. His research interest is equipment system network.

Yong Gang Li graduated from Shanghai Jiao Tong University in 2007 with a ph. D. degree in communication and information systems. From 2012 to 2013, he was a visiting scholar in the Department of Electronic Engineering, University of Wisconsin-Madison, engaged in large-scale network signal processing research. His research interest covers network complexity, tactical communication network simulation, network security, and network visualization.

Ying Wang graduated from Cangzhou Normal University with a bachelor's degree in Communication Engineering in 2019. She is currently pursuing a master's degree in school of communication and information engineering at Chongqing University of Posts and Telecommunications in Chongqing, China. His research interest is equipment system network.