Research of Anti-destroy Optimization in Combat System Complex Network Based on Fractal Theory

Deng Qing\(^1\), Xue Qing\(^1\), Chen Lin\(^1\) and Yu Ping-Gang\(^2\)

\(^1\) Army Armored Force Institute, Beijing 100072, China;
\(^2\) National Defence University of PLA, Beijing 100091, China

154247597@qq.com

Abstract: Studying anti-destroy forecast of combat system complex network, which is of great resisting damage and improving survival ability. Optimizing the network anti-destroy, it may change the system into network composed of nodes and routes, measure network connection with intercommunication and the shortest path length to optimize anti-destroy property. Traditional methods improve network by increasing or decreasing side and get less center node and more collect ratio, but ignore command grade of combat system and affect forecast result. The article proposes a method for optimizing the network anti-destroy based on fractal theory. The network is constructed by case calculation means of fractal dimensionality. According to the connect way of relevance hybrid dimensionality and plus-minus related, the thesis realized fractal optimization of existing system network based on isolating colony node and extending path. By simulation test, the method can effectively improve network anti-destroy property.

1. Introduction

With the information technology continuous development and extensive use in the military field, the composition of combat systems has become increasingly complex, interrelated and influenced each other. The combat effectiveness has increasingly depended on the overall combat capability formed by close cooperation with each other. In actual war, the combat system is under the enemy's random and selective attack. It is of great military value enhancing the combat capability of the combat system to grasp the initiative on the battlefield and win the war. Existing research shows that combat systems reflect the small-world, scale-free features of complex networks [1]. Therefore, how to optimize the anti-destroy of the combat systems complex network and find out the key node or connection has become an important issue to be solved [2, 3].

At present, the main method of research on anti-destroy in combat system complex network is mainly based on the study of complex network invulnerability. Also it has obtained some research findings. For example, in literature [4], the problem of network anti-destroy is converted into seepage of a generalized random graph. Using the more general origin function method, it random gave the critical value of removal ratio under failure condition. There is only one selective attack type in the network failure mode of this method, which is not completely consistent with reality. In literature [5], tabu search algorithm is used to study the invulnerability optimization of complex networks with arbitrary degree distribution. In the process of invulnerability optimization, the network efficiency is taken as the objective function, and the mean value of the network degree distribution is used as cost constraint to construct optimization model with optimal network topological structure. The algorithm can search for the optimal network structure with given cost constraints in the topological network.
space of the current network and the global coupling network, but there may be a problem of getting into a local optimum.

In view of the existing problems above, a method based on fractal theory is proposed to optimize the invulnerability of the combat system complex network on the basis of summarizing relevant literatures. The experimental results show that the proposed method can effectively improve the destruction resistance.

2. Fractal Characteristic of Combat System Complex Network

In the process of optimizing the invulnerability of combat system complex network, the combat system is transformed into a complex network according to complex network theory. Evaluation index of damage resistance is selected to analyze the invulnerability of different degree distribution networks against different strike modes, which can realize the invulnerability optimization of the combat system complex network. The specific process is as follows:

In the military system, due to the demand of operational command and control, combat system formed a top-down and hierarchical structure[6-7]. This hierarchical network can be seamlessly integrated into a scaleless topology. It has a fixed module structure and the power degree index is as follows:

\[ \gamma = 1 + \frac{\ln 4}{\ln 3} = 2.26 \]  

The most important feature of above modular level network is agglomeration factor:

\[ C(k) \approx k^{-1} \]  

The curve of function C(k) is a straight line with a slope of -1 in the double logarithmic coordinate system. The hierarchical network structure means that sparsely connected nodes are part of a highly connected clustered area and communicate connections among highly connected clusters, which are composed of cluster nodes. The self-similar feature presented by the combat system complex network lays the foundation for the application of the invulnerability of the combat system complex network.

Based on above characteristics, a combat system complex network model is constructed. For any combat system G, the nodes of system are composed of targets, reconnaissance, accusations, and blows. The interconnected edges are consisted of single combat system network information flow and energy flow against enemy, with directed edges. These nodes and edges form a complex network model of combat system. Its formal representation is:

\[ G = (P, L) \]  

\[ P \in [P_t \cup P_o \cup P_c \cup P_f] \]  

\[ L \in [L_t \cup L_o] \]  

In the formula, \( P_t, P_o, P_c, P_f \) respectively represent the target, reconnaissance, accusation and attack node. \( L_t, L_o \) represents single communication network information flow and energy flow against enemy.

Anti-destroy of complex network refers to the ability of the network to maintain its functions under the condition that nodes or edges in the network are naturally defeated or deliberately attacked. In the combat system complex network, this ability maintaining its function is mainly reflected in the ability of the topology structure to hold connectivity. Therefore, the anti-destroy of a complex network is mainly due to the redundancy of alternative approaches between nodes, including concepts of efficacy and vulnerability. For the efficiency of the network, the network's average shortest path CPL, diameter D, clustering coefficient C are used to measure effectiveness of the network.

\[ CPL = \frac{1}{N(N+1)/2} \sum_{i,j} d_{ij} \]  

\[ N \] is the total number of nodes, and \( d_{ij} \) is the shortest path between nodes i and j.

\[ D = \max_{i,j} d_{ij} \]
\[ C = \frac{1}{n} \sum_{i=1}^{n} \frac{E_i}{k_i(k_i - 1)/2} \]  

In the formula, \( n \) is the total number of nodes, \( k_i \) is the neighbor node of node \( i \), and \( E_i \) is the number of edges actually existing among \( k_i \) neighbor nodes.

The vulnerability of network is related to decrease of network performance after some nodes or edges in the network are attacked. The critical value \( f_c \) of the node removal ratio of network collapse is used to calculate the network vulnerability.

\[ f_c = 1 - \frac{1}{\kappa_0^2 / \kappa_0 - 1} \]  

\( \kappa_0 \) is the degree distribution of the initial network.

3. Anti-destroy Optimization of Combat System Complexity Network Based on Fractal Theory

3.1 Algorithm Principle

In the process of the anti-destroy optimization of the combat system complex network, the important concept that characterizes the fractal characteristics of the combat system complex network is the fractal dimension \( d_B \), and the box counting method[8] is used to calculate the fractal dimension. The specific steps are detailed as follows:

First, all the network nodes are covered with a box of size \( S_B \). The information such as Euclidean distance between network nodes is not considered here, and only the shortest path length between abstract extracted nodes is considered. All nodes covered by a box are connected to each other with a minimum distance smaller than the box scale \( S_B \). Then a node is used to represent a box in the newly constructed network, which can obtain the minimum number of boxes \( N(S_B) \) to cover the network.

According to existing research, the actual complex network (in Figure 1) is calculated using the box counting method:

\[ N(S_B) \log(S_B) \approx d_B \]  

\[ \frac{N(S_B)}{N} \approx S_B^{-d_B} \]  

Figure 1. \( N(S_B) \) Logarithm of network.

Transforming different box sizes, renormalize the network and give new connection probability distributions. Obviously, because there is no change in the complex network, only the method of representation is different, the scale of its degree distribution remains invariant.

\[ \begin{align*}
    P(k) &\approx k^{-\gamma} \\
    P(k') &\approx (k')^{-\gamma}
\end{align*} \]  

From Figure 1, we can see that in the real-world network, there is a relationship between scale factor \( S_B \) and \( d_B \):

\[ I(S_B) \approx S_B^{-d_B} \]  

From the renormalization process of www network as shown in Figure 2, there is a relationship between the degree \( k' \) of the nodes in the network after renormalization and the maximum number \( k \) of connections with each box:

\[ k' = I(S_B)k \]
Suppose \( n(k) \) denote the number of nodes with a degree \( k \) in the network before renormalization.

\[
n(k) = N P(k)
\]  

(14)

\( n'(k') \) denotes the number of boxes with moderate \( k' \) in the network after renormalization.

\[
n'(k') = N P(k')
\]  

(15)

Since the network was renormalized, its structure did not change.

\[
n(k) d k = n'(k') d k'
\]  

(16)

Substitute formula (12)

\[
n(k) d k = n'(k') d k' = n'(I k) d (I k)
\]  

(17)

Substitute formula (14)

\[
N P(k) d k = N' P(I k) d (I k)
\]  

(18)

Substitute formula (10)

\[
N = N' I^{1 - r}
\]  

(19)

Substitute formula (2)

\[
d_b = (r - 1) d_k
\]  

(20)

From formula (20), if \( r > 1 \), then \( N(S_b)/N \) obeys power-law distribution, and the entire complex network presents fractal features; conversely, if \( r < 1 \), \( N(S_b)/N \) obeys exponential distribution, complex network it presents a non-fractal characteristic. This provides assurance for us to achieve the goal of improving the destruction resistance of combat system complex networks by changing the topological structure of the complex network.

### 3.2 Optimization Model

In the course of the invulnerability optimization of the complex network of combat systems, based on the fractal dimension, the network growth rules are determined according to the fractal theory and the growth equation is obtained. Then use the degree of node negative correlation to achieve network reconstruction and optimize the network anti-destroy. The detailed steps are described as follows:

The connection relationship between cluster nodes of a complex network determines that complex networks exhibit different characteristics. If the connection relationship between the cluster nodes is positively related, that means the cluster nodes in the network tend to connect with other cluster nodes, as a whole the network presents a small-world feature; conversely, if there is a negatively correlated connection relationship between the cluster nodes, the cluster nodes are more likely to connect to non-cluster nodes with less connectivity, the network exhibits self-similar fractal features. In other words, weak negative correlation or irrelevant growth mechanisms lead to the characteristics of non-fractal topologies[9]. It can be seen that any kind of complex network is determined to exhibit fractal characteristics as connection strength between cluster nodes.

Evolve the growth process by time and build an improved combat system model as follows:

![Figure 2. P(k) Logarithm of network.](image)
1) Build initial network. Assuming that the initial network is a star network, the total number of node is \( n(0)=5 \), and the number of edge \( k(0)=4 \). Each initial node becomes a cluster node with time.

2) Network growth rules. Suppose every new time step, add \( h(t-1) \) new nodes to nodes with degree \( k(t-1) \). Growth equation of the network can be expressed:

\[
 n(t) = n(t-1) + 2hk(t-1)
\]  

(21)

Without considering ring structure, then:

\[
 k(t-1) = n(t-1) - 1
\]  

(22)

By equations (21), (22)

\[
 \lim_{t \to \infty} \frac{n(t)}{n(t-1)} = 2h + 1
\]  

(23)

It can be seen that the structure presented by the entire network has nothing to do with the initial structure of the network with the continuous growth of the network. Therefore, the initial structure of network can not determine the characteristics of the final network.

3) Reconnection rules of the network. There are two different network reconnection rules

Rule-1: any two boxes are directly connected to the cluster node by the probability \( p \) through the cluster nodes in the box. The network is reconnected according to the degree of positive correlation of the nodes;

Rule-2: Any two boxes are connected through a non-cluster node in the box with a probability of \( 1-p \), that means they are reconnected to the network according to the negative correlation of nodes.

From the different reconnection principles above, it can be seen that Rule-1 will cause the network to exhibit high clustering and short-path characteristics of small-world features; on the other hand, Rule-2 leads to cluster nodes separation in the network. the path becomes longer, the network gradually presents a fractal feature. The simultaneous appearance of small-world features and fractal features in real networks is due to the different combinations of two different growth models. Figure 3 shows the network growth model under two different time evolution mechanisms.

![Network Growth Models](image)

(a) Initial network, (b) Rule-1, (c) Rule-2, (d) Rule-1 & Rule-2

Figure 3. Two different network growth models.

4. Simulation Test

In order to prove the effectiveness of the proposed method based on fractal theory, an experiment is needed. The experiment adopts the object-oriented programming method and uses VC++ development environment and Matlab simulation tools to simulate. In the experiment, a complex network of two groups of combat systems is constructed. Assume that the reconnaissance nodes that make up each team are composed of reconnaissance and detection devices that are assigned to them, specifically two...
battlefield televisions, three-step tactical radars, three light armored reconnaissance vehicles, and two aircrafts. Unmanned reconnaissance aircraft, a total of 10 nodes; command and control unit consists of 4 battalion command vehicles and 1 regiment command post, a total of 5 alleged nodes; the strike unit consists of 4 tank companies, 8 machine companies, and 3 artillery units. Even composed, a total of 15 combat nodes; then the two missions cooperative combat system has a total of 20 reconnaissance nodes, 10 alleged nodes, 30 cracked nodes, and 30 target nodes.

The complex network model of the two groups of combat systems is reconnected based on fractal theory. The changes of anti-destroy index are shown in Table 1:

| Efficiency | Vulnerability |
|------------|---------------|
| **Anti-destroy CPL D C f** | **<C>** |
| Before fractal optimization | 2.238 | 6 | 0.67 | 0.022 |
| After fractal optimization | 2.243 | 7 | 0.56 | 0.082 |

From table 1, we can analyse the efficiency index of anti-destroy. The length of the average shortest path increases slightly after fractal optimization. The network diameter also increases from 6 to 7, which shows that the response speed of combat system complex networks has slightly decreased. Because the path passing among nodes becomes long after the cluster node is reconnected.

From the vulnerability index of anti-destroy, it is difficult to compare the differences between the two networks because of small scale. So we magnify ten times, using a focused attack method which is based on the degree of the cluster node and remove node one by one. In this case, we can find the rule of the maximum cluster C, average value <c>[10] and removal ratio f. The results are shown in figure 4 and 5.

![Figure 4. Curve of maximum cluster C with removal ratio f.](image)

![Figure 5. Curve of average value <c> with removal ratio f.](image)

From Figures 4 and 5, it can be seen that when the proportion of cluster nodes are removed from the network, f = 0.022, the current maximum cluster C of the complex network with non-fractal combat systems has fallen to zero, while the complex network with fractal combat systems, f=0.082, it drops to 0; similarly, when the proportion of cluster nodes are removed from the network, f=0.022, average value <c> of the complex network with non-fractal combat systems has risen to near the peak value. However, the fractal battle system complex network rose to its peak value about f=0.082. we
can draw a conclusion that the fractal combat system complex network has significantly stronger
destruction resistance than other battle system complex networks under the same condition and.

5. Conclusions
Based on the fact of the self-similar fractal feature in the actual complex network and the
characteristics of hierarchical networks in the combat system structure, this paper proposes an
anti-destroy optimization method for combat system complex network based on fractal theory.
Through simulation test and insurability comparison, it is proved that the optimized combat network
has a high resistance to destruction as a whole.

References
[1] David.A.Jarvis. a methodology for analyzing complex military command and control(C2)
networks[R]. in the 10th International Command and Control Research and Technology
Symposium. 2005. U.S.A.
[2] Wang B, T.H.W., Guo C.H, etc, Entropy Optimization of Scale-free Networks Robustness to
Random Failures[J]. Physica A, 2005. 363: p. 591-596.
[3] Wang Bing, T.H., etc, Optimization of network structure to random failures[J]. Physica A, 2006.
368: p. 607-614.
[4] Wang Bing, T.H., etc, Optimization of network structure to random failures[J]. Physica A, 2006.
368: p. 607-614.
[5] Callaway D S,Newman M E J,Strogatz S H,et al. Network robustness and fragility:percolation
on random graphs[J]. Phys.Rev.Lett.,2000,85(25):5468-5471.
[6] Han Zhu, Jianyang Zhu. Network architecture [J]. Physics, 2003. 32(6): p. 364-369.
[7] Ravasz E, B.A.L., Hierarchical organization in complex networks[J]. Physical.Review.Lett,
2003. 67: p. 026112.
[8] Chaoming Song, S.H., Hernan A, Makse Self-similarity of complex networks[J]. Nature 2005.
433: p. 392-395.
[9] Chaoming Song, S.H., Hernan A, Makse. Origins of fractality in the growth of complex
networks[J]. Nature 2008. 433: p. 382-386.
[10] Albert R, J.H.B.A.L., Attack and error tolerance in complex networks[J]. Nature, 2000. 406: p.
378-382.