Information Sciences 426 (2018) 148–159

Contents lists available at ScienceDirect

Information Sciences

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

Measure of invulnerability for command and control network based on mission link

Wang Yunming[a,b,*], Chen Si[b], Pan Chengsheng[b], Chen Bo[b]

[a] School of Automatic, Nanjing University of Science and Technology, Nanjing, 210094, China
[b] School of Information Engineering, Dalian University, Liaoning, 116622, China

ARTICLE INFO

Article history:
Received 17 April 2017
Revised 13 October 2017
Accepted 15 October 2017
Available online 16 October 2017

Keywords:
C2 network
Invulnerability
Super network theory
Mission link efficiency
Mission link entropy

ABSTRACT

In Command and Control (C2) network, the measure of invulnerability mainly focuses on structural characteristics of the network, where the operational mission has not been adequately considered. As a result, it becomes difficult to assess the invulnerability of C2 network in a dynamical manner. In this paper, the operational entities and heterogeneous relationships among combat entities are analyzed, where the operational C2 network model is constructed based on the combat theory of OODA and the super network. Subsequently, the mission link is defined, which can be used to characterize the combat network. Finally, a new measure of invulnerability for C2 networks is proposed based on the efficiency and entropy of the mission link. In particular, this measure can desirably represent the efficiency of information transmission and robustness of network structures, respectively. The simulation results have demonstrated that the proposed invulnerability measure is highly sensitive and accurate. More specifically, the proposed measure could more accurately reveal the invulnerability of C2 network, where theoretical basis for designing and optimizing the structure of C2 networks can be also provided.

1. Introduction

In information warfare, the C2 network plays an essential role in achieving superiority in information, which is helpful in decision-making process and will lead to better battle operations ultimately. On the one hand, C2 networks can connect the systems such as the early-warning detection system, the command and control system, and the firepower system etc. On the other hand, C2 networks can provide important guarantees for effective and synchronized operations [28]. The complex and diverse relationships among the elements of C2 networks have changed the major factors affecting the invulnerability for C2 networks, including the functionality and performance of elements and the system structure morphology of elements. However, failure of nodes or edges in C2 networks will often be caused by attacks, where the original network topology would become dividing and even lead to the damage of the global network [11]. If the C2 network is under attack, it remains to be an active research area to measure the invulnerability of C2 networks by evaluating the overall combat efficiency and complete combat mission [1,17].

Since the structure of C2 networks has transformed from the pyramid type to the type of flexible recombination and random access, various investigations have been performed for modeling network structures, invulnerability and robustness

* Corresponding author.
E-mail addresses: wang19871128@126.com (W. Yunming), free19910201@126.com (C. Si), pancs@sohu.com (P. Chengsheng), chenbo20040607@126.com (C. Bo).

https://doi.org/10.1016/j.ins.2017.10.035
0020-0255/

in C2 networks [29]. In general, the research of network invulnerability can be divided into two categories, i.e., graph theory and statistical physics. The graph theory based research primarily analyzed the invulnerability of the network, where measures including connectivity, toughness, integrity, tenacity, dispersion and nuclear were considered. These measures could be highly accurate; however, these methods were NP hard problems. Therefore, it is not even possible to apply these measures to large-scale C2 networks [36].The statistical physics base invulnerability measures were initially proposed by Albert [2]. The researchers have recorded the change of the network performance with removal of nodes or edges by various simulations of complex networks. In this way, the invulnerability of the network can be achieved. Based on this methodology, many researchers have evaluated the network performance from perspectives of information transmission efficiency and structural robustness [16].

These evaluation measures are based on the efficiency of information transmission including network diameter, average diameter, average path length, network efficiency and so on. Bian [3] has proposed an efficient algorithm for calculating the average diameter in the investigation of the minimum path graphs of directed double loop networks. In this work, the relationship between the network diameter and the average diameter was simulated. It has been concluded that the average diameter should be a better measure than the network diameter in evaluating the efficiency of network transmission. In [36], a class of algorithms were proposed to evaluate the network transmission efficiency. This method was able to effectively calculate the betweenness centrality and the average path length of a dynamic network. In [37], the efficiency of network was redefined to measure the efficiency of information transmission for multi-class network, where time-based decision criterion (TBDC)and monetary-based decision criterion (MBDC) standards were used to measure the validity and effectiveness of this index. Moreover, it was demonstrated that the index was very effective. In [38], a performance evaluation method was proposed, where Monte Carlo simulations were carried out based on network model to validate the reliability. In particular, a graph transformation based method was proposed to reduce the performance of protective measures, which could substantially reduce the complexity of network performance evaluation.

The structural robustness based on evaluation indexes mainly consist of the maximum connected subgraph, algebraic connectivity, natural connectivity and network structure entropy. In [18], a network robustness measure was proposed based on a maximal connected subgraph, where the robustness of networks was evaluated under all kinds of attacks, such as random attack, degree rank attack, betweenness rank attack. In [6], weighted algebraic connectivity was employed to analyze the robustness of network structure with uncertain disturbance. This work concluded that the high density of nodes posse would induce more connection and usage, which could become more unreliable. In [32], natural connectivity was proposed to characterize the structure robustness of complex network, which could measure network connectivity with the redundant paths between nodes. This method was able to validate natural connectivity by comparing with other structural robustness parameters. In [12], network structure entropy was used to measure the order and stability of supply chain system, which could be used to analyze the influences of network scale and node connection probability on the stability of system structure. It should be noted that the research on the invulnerability of C2 network is still in its initial stage. In [36], the invulnerability of combat network was investigated based on the connectivity of nodes and edges, where average path length was employed to simulate the relationship between the network structure and the efficiency of network operations on the combat unit. This study concluded that the network average distance was an effective index to measure network-centric warfare, where the essential idea was to employ the traditional measure in complex networks. However, no special attention has been paid to the applicability of C2 network. From this perspective, the Perron-Frobenius eigenvalue (PFE) of adjacency matrix is often used in most representative work to measure network performance of the Information Age Combat Model (IACM), which has been introduced by Cares etc. in [5]. Although this idea is proposed, the specific application of IACM has not been adequately investigated, where the validity of PFE and other problems has also not been validated By theoretical derivation or experimental verification. In [7–8], research was further carried out based on Cares's IACM theoretical model, where simulation was also carried out based on Netlogo. This study preliminarily validated PFE as an evaluation index measure for operational effectiveness of a network. The simulated experiments suffered from various limitations. For example, decision nodes were not connected to the network, the network scale was too small or the difference of node's own capability was not adequately considered.

In this paper, the structural and functional properties of the C2 network are extensively investigated. Based on the super network theory and the combat theory of Oberve-Orient-Decide-Act (OODA) [19–20], all types of combat entities and communication links between entities can be characterized as nodes and edges, respectively. In particular, a typical C2 network model can be constructed based on the super network. In this work, the concept of mission link is introduced and the calculation method of the number of mission link is proposed. Subsequently, two invulnerability measures are proposed based on efficiency and entropy of mission link, where the network invulnerability can be evaluated from the perspectives of information transmission efficiency and network structural robustness. Finally, the invulnerability of C2 network is analyzed with extensive simulation results.

2. Super network model for C2

In general, C2 super network is a multi-layer and multi-edge heterogeneous network [4,34], which can be constructed by connecting different kinds of operational nodes in a certain order and interconnecting different functional networks. This is based on various relationships of information, where the demand of combat mission can be satisfied. Based on certain

mapping rules, a super network model can be constructed, where various types of combat nodes can be connected with each other by the relationships among intelligence information, C2 information and fire information [21].

2.1. Abstraction of operational node

Base on the OODA loop, the operational nodes can be categorized into sensing nodes, C2 nodes and fire strike nodes. It is assumed that the total number of nodes is N, the number of sensing nodes is n, the number of C2 nodes is m, and the number of fire strike nodes is t, where the equality $N = n + m + t$ should be satisfied. Each category of nodes consist of its own properties, and the ith node can be given as

$$N(i) = \{ID_N(i), T_N(i), P_N(i), H_N(i), GD_N(i), C_N^*(i), I_N^*(i), F_N^*(i)\} \tag{1}$$

where $ID_N(i)$ represents the sequence number of the ith node, $T_N(i)$ represents the type of the ith node, $P_N(i) = \{P_1, \ldots, P_m\}$ represents the capability of the ith node to process all types of information, $H_N(i)$ represents the hierarchy of the ith node, $GD_N(i)$ represents the location of the ith node, $C_N^*(i)$ represents a set of C2 nodes connected to the ith node, $I_N^*(i)$ represents a set of sensing nodes connected to the ith node and $F_N^*(i)$ represents a set of fire strike nodes connected to the ith node.

(1) The Sensing node is the combat unit, which is capable of providing early warning, detection, reconnaissance and monitoring [39]. Examples of sensing nodes include early-warning radar, reconnaissance radar and so on. The main functionalities of these sensing nodes are to obtain intelligence information on battlefields and acquire evaluation information on operational effects. In particular, the information collected by sensing nodes will be transmitted back to C2 nodes. The ith sensing node can be expressed as

$$\begin{aligned} &N_I(i) =< ID_I(i), T_I(i), C_I(i), H_I(i), GD_I(i), C_I^*(i) > \\ &ID_I(i) \in [1, n] \end{aligned} \tag{2}$$

(2) C2 node is the operational units with the capability of information fusion, command decision making, information coordination and distribution. Examples include command bodies, information processing bodies. The ith C2 node can be expressed as

$$\begin{aligned} &N_C(i) =< ID_C(i), T_C(i), C_C(i), H_C(i), GD_C(i), C_C^*(i), I_C^*(i), F_C^*(i) > \\ &ID_C(i) \in [n{+}1, n + m] \end{aligned} \tag{3}$$

(3) Fire strike node is the operational unit which is capable of interception and attacking. Examples include various types of air defense weapons. The ith fire strike node can be expressed as

$$\begin{aligned} &N_F(i) =< ID_F(i), T_F(i), C_F(i), H_F(i), GD_F(i), C_F^*(i) > \\ &ID_F(i) \in [n + m{+}1, N] \end{aligned} \tag{4}$$

2.2. Operational relationship abstraction

The connection among cable-connected operational node, communication equipment and other physical means of communication is defined as the operational relationship. For the purposes of interactive processing of different types of information, these connections are able to achieve intelligence, commanding, firing and information transmission among nodes [13]. Based on various types of functionalities of the nodes and their interactions with others, the operational relationship can be summarized into three categories, namely, the relationships between sensing nodes and C2 nodes, among C2 nodes, and between C2 nodes and fire strike nodes. This interactive relationship between node i and node j can be expressed as

$$E_{i,j} =< R(i, j), D(i, j), A(i, j) > \tag{5}$$

where $R(i, j) =< R_{I,C}(i, j), R_{C,C}(i, j), R_{F,C}(i, j) >$ denotes the connection relationship among nodes. If sensing node v_i and C2 node v_j are interactively correlated, $R_{I,C}(\mathrm{i,j}) = 1$; otherwise, $R_{I,C}(\mathrm{i,j}) = 0$. Moreover, $D(i, j)$ represents the direction of the heterogeneous edge, where $D(i, j) = \{-1, 0, 1\}$. More specifically, $D(i, j) = 1$ represents the edge direction from node v_i to v_j, $D(i, j) = 0$ indicates no direct edge direction between node v_i and v_j, and $D(i, j) = -1$ represents the edge direction from node v_j to v_i. Moreover, $A(i, j)$ is the identification of attributions, which includes the attributes such as information, delay, bandwidth, and link-length. In particular, it can be expressed as $A(i, j) = \{A_{i,j}^{(1)}, A_{i,j}^{(2)}, \ldots, A_{i,j}^{(n)}\}$, where n is the number of attributions and $A_{i,j}^{(k)}$ is the kth attribute value of the link between the node v_i and v_j, $k \in [1, n]$.

(1) The interactive relationship between the sensing node and the C2 node represents the interactive relationship between sensing nodes and C2 nodes. This relationship can be characterized by the process of information which is detected by sensing nodes distributed to each operational node. More specifically, it is formulated as

$$E_{I,C}(i, j) =< R_{I,C}(i, j), D_{I,C}(i, j), A_{I,C}(i, j) > \tag{6}$$

(2) The interactive relationship among the C2 node represents the interactive relationship among C2 nodes. This relationship can be formed by the process of complete the order issued, resource sharing, information collaboration among C2 nodes, which is formulated as

$$E_{C,C}(i, j) =< R_{C,C}(i, j), D_{C,C}(i, j), A_{C,C}(i, j) > \tag{7}$$

(3) The interactive relationship between the c2 node and fire strike node represents the interactive relationship between C2 nodes and fire strike nodes. This relationship can be obtained by the process of orders issuing from C2 nodes to fire strike nodes, which is formulated as

$$E_{F,C}(i,j) =< R_{F,C}(i,j), D_{F,C}(i,j), A_{F,C}(i,j) > \tag{8}$$

2.3. C2 super network model

Based on the theory of super network [14,30] and abstract of nodes and edges in the C2 network, three kinds of networks can be formed to the C2 network, the sensing network and the fire attacking network. Therefore, the super C2 network model can be described by $G_{C^2N} = (G_{I-C}, G_{C-C}, G_{C-F})$. This model is obtained by combining the three relation matrices as follows,

$$G_{C^2N}=\begin{matrix} \\ I \\ C \\ F \end{matrix}\begin{matrix} \begin{matrix} I & C & F \end{matrix} \\ \begin{bmatrix} 0 & G_{I-C} & 0 \\ G_{I-C} & G_{C-C} & G_{C-F} \\ 0 & G_{C-F} & 0 \end{bmatrix} \end{matrix} \tag{9}$$

where G_{I-C} represents the sensing network formed by the interactive relationship between sensing nodes and C2 nodes, $G_{C\text{-}C}$ represents C2 network formed by the mutual interleaving of various types of C2 nodes at different levels, and G_{C-F} represents fire attacking network formed by the connection of C2 nodes and fire strike nodes.

In particular, each network can be represented by $G = G(N, E)$, where N is the abstraction of the operational node and E is the abstraction of the relationship among the operational nodes.

3. Measure of invulnerability based on mission link

3.1. Mission link efficiency

The time efficiency of an operation is crucial to convert information superiority to operational superiority, which is also the basis for each every element in operational element. With time efficiency, the combat effectiveness and synchronization operations synchronization can be obtained [9]. In this sense, the combat efficiency is an important criteria criterion to measure the invulnerability of C2 network. In general, the network efficiency is often employed to measure the effectiveness of information transmission in complex networks. In the C2 network, however, the node is heterogeneous and hierarchical, where the efficiency of conventional network cannot be straightforwardly employed as a measure of operational rate combat speed [27]. It is necessary to incorporate the characteristics of C2 network for measuring the information efficiency, which can be mission-oriented combat. Based on the characteristics of OODA combat process and combing the network efficiency in complex network, a new measure is proposed to evaluate the invulnerability for C2 network based on the mission link. In general, more efficient mission link would obtain better operational performance of the network [16].

Definition 1. Mission link. One or more detection- command-attack integrative link is defined as mission link, which is formed by information flow from sensing nodes to strike nodes via C2 nodes during the combat process. The mission link has the characteristics of time sequence, direction and so on.

Definition 2. Efficiency of Mission link. The average value of the maximum efficiency for all mission links between sensing nodes and fire attacking node is defined as

$$E_{gcl} = \frac{1}{L}\sum_{i=1}^{n}\sum_{j=n+m+1}^{N}\frac{1}{d_{O_iF_j}} \tag{10}$$

where n denotes the number of sensing nodes, m denotes the number of fire attacking nodes, $d_{O_iF_j}$ denotes the shortest path from node O_i to node F_j, O_i denotes the ith sensing node, F_j denotes the jth fire strike node and L denotes the number of mission link.

Moreover, L can be computed via $n_{ij}{}^{l}$, given that $n_{ij}{}^{l}$ is defined as the number of closed walks with a distance of l between the sensing node O_i and F_j. In addition, the formulae of L could be expressed as

$$L = \sum_{i=1}^{n}\sum_{j=n+m+1}^{N}\sum_{l=0}^{\infty} n_{ij}{}^{l} \tag{11}$$

However, when l is infinite, the computation of L would subsequently become massive and highly complex. Consequently, a closed walks based method for calculating the number of mission links is proposed in this paper, which tackles the computation problem. In particular, a closed walk is constructed by connecting the sensing node O_i and fire strike node F_j. Furthermore, the node O_i represents both starting point and end point [22]. Subsequently, the number of mission links would be equal to the number of closed walks. Therefore, let G'_{C^2N} denote the new network constructed in this method.

Assume that n_i^l represents the number of closed walks with the distance of l, where the node O_i represents both starting point and end point. Subsequently, a simplified form of (2) can be obtained

$$L = \sum_{i=1}^{n}\sum_{l=0}^{\infty} n_i^l = \sum_{l=0}^{\infty}\sum_{i=0}^{n} n_i^l = \sum_{l=0}^{\infty} n_l \tag{12}$$

where n_i^l denotes the number of closed walks with the distance of l starting from sensing nodes to C2 nodes and the fire strike node. As $l\to\infty$, the length of closed walks would become indeterminate. To ensure the convergence of L, $1/l!$ is determined to be the weight of n_l. Moreover, the total number of closed walks could be expressed by L' equivalently

$$L' = \sum_{l=0}^{\infty} \frac{n_l}{l!} \tag{13}$$

where n_{ij}^l represents the number of closed walks with the distance of l between node v_i and node v_j. It should be noted that the matrix A^l is constructed using n_{ij}^l, where the diagonal element a_{ii}^l represents the number of closed walks with the length of l via node v_i. In addition, the following expressions can be obtained

$$\sum_{i=1}^{N} n_{ii}^{(l)} = trace(A^l) = \sum_{i=1}^{N} \lambda_i^l \tag{14}$$

$$\sum_{i=1}^{N} n_{ii}^{(l)} = \sum_{i=1}^{n} n_{ii}^{(l)} + \sum_{i=n+1}^{n+m} n_{ii}^{(l)} + \sum_{i=n+m+1}^{n+m+t} n_{ii}^{(l)} \tag{15}$$

where $\sum_{i=n+1}^{n+m} n_{ii}^{(l)}$ denotes the number of closed walks with the length of l and C_i being the starting point. It should be noted that the number of closed walks consists of two parts. In the first part, the number of closed walks with the length of l only refers to C2 nodes. Moreover, it is equivalent to compute all numbers of closed walks with the distance of l in the graph G_{C-C} and denote the number by $L_{G_{C-C}}$. In the second part, it is assumed that n_l is the number of closed walks with the distance of l, starting from the C2 node C_i to the fire strike and sensing nodes. Therefore, the following expression can be obtained

$$\sum_{i=1}^{N} n_{ii}^{(l)} = \sum_{i=1}^{N} \lambda_i^l = 3n_l + L_{G_{C-C}}. \tag{16}$$

According to (16), we can obtain,

$$L_{G_{C-C}} = \sum_{j=1}^{m} n_{jj}^{(l)} = \sum_{j=1}^{m} {\lambda'}_j^l. \tag{17}$$

Substituting (17) into (18), it can be obtained,

$$n_l = \frac{\sum_{i=1}^{N} \lambda_{i^l} - \sum_{j=1}^{m} \lambda'_{j^l}}{3}. \tag{18}$$

Substituting (9) into (4), it can be further obtained,

$$\begin{aligned} L' &= \sum_{l=0}^{\infty} \frac{\sum_{i=1}^{N} {\lambda_i}^l - \sum_{j=1}^{m} {\lambda'}_j^l}{3l!} = \frac{1}{3}\left(\sum_{i=1}^{N}\sum_{l=0}^{\infty} \frac{{\lambda_i}^l}{l!} - \sum_{j=1}^{m}\sum_{l=0}^{\infty} \frac{{\lambda'}_j^l}{l!}\right) \\ &= 1/3\left(\sum_{i=1}^{N} e^{\lambda_i} - \sum_{j=1}^{m} e^{\lambda'_j}\right) \end{aligned} \tag{19}$$

where λ_i and λ'_j denote the eigenvalues of the adjacency matrices G'_{C^2N} and G_{C-C} respectively. Followed the expressions above, the efficiency of mission links E'_{gcl} could be calculated by

$$E'_{gcl} = \frac{3}{\left(\sum_{i=1}^{N} e^{\lambda_i} - \sum_{j=1}^{m} e^{\lambda'_j}\right)} \sum_{i=1}^{n} \sum_{j=\mathrm{n+m+1}}^{N} \frac{1}{d_{O_i F_j}}. \tag{20}$$

3.2. Entropy of mission link

In general, the stability and integrity among combat entities essentially guarantee all operational elements. In particular, they could mutually coordinate and fully contribute to the overall combat performance [33]. In order to compromise the stability of the enemy's network structure, attacking key nodes and links is the most common strategy in the war [23,31]. According to the complex network theory, the stability and integrity of a network can be measured via entropy. In addition, measuring entropy is to measure the uniformity of the energy's distribution in a system. Meanwhile, entropy indicates whether the state of an object is stable, which could also indicate the changes of direction in the system. In fact, an energy distribution closer to uniform distribution could cause a larger entropy value and vice versa. Many researches have concluded that C2 networks share the same characteristics as complex networks. In particular, the scale-free feature is one of the common characteristics, where only a small number of nodes are critical. Moreover, for a C2 network under deliberate attacks, less obvious critical nodes could improve the invulnerability for the C2 network; however, under random attacks, more obvious critical nodes could lead to the better invulnerability of the C2 network.

(1) The betweenness of mission link

In complex networks, the node betweenness is defined as the proportion of the shortest path number via the current node to the total shortest path number. Moreover, the betweenness is also a global variable indicating the functionality and effect of a node or an edge in the network [24,40]. According to the definition of betweenness and the nodes' characteristics in C2 networks, the node mission link betweenness is involved in this paper. In other words, this concept is defined as the proportion of the shortest mission links via the current node to all shortest mission links. Thus, the node mission link betweenness could be calculated as

$$b_c = \frac{\sum_{i=1}^{n}\sum_{j=n+m+1}^{N} m_c(O_i, F_j)}{\sum_{i=1}^{n}\sum_{j=n+m+1}^{N} m(O_i, F_j)} \quad (i \neq j \neq c) \tag{21}$$

where b_c denotes the mission link betweenness of the node v_c, $m(O_i, F_j)$ denotes the number of shortest paths from the sensing node O_i to the fire strike node F_j, and $m_c(O_i, F_j)$ denotes the number of shortest paths from the sensing node O_i to the fire strike node F_j via the node v_c.

In a similar manner, the mission link betweenness of the edge b_{gl} could be defined as the proportion of the shortest path number via the current edge to the total shortest path number. Therefore, the node mission link betweenness could be calculated as

$$b_{gl} = \frac{\sum_{i=1}^{n}\sum_{j=n+m+1}^{N} m_{e_{gl}}(O_i, F_j)}{\sum_{i=1}^{n}\sum_{j=n+m+1}^{N} m(O_i, F_j)} \quad (i \neq j \neq l \neq g) \tag{22}$$

where $m(O_i, F_j)$ represents the shortest path number from the sensing node O_i to the fire strike node F_j, and $m_{e_{gl}}(O_i, F_j)$ represents the shortest path number from the sensing node O_i to the fire strike node F_j via the edge e_{gl}.

It should be noted that the mission link betweenness indicates the significance of nodes or edges in the C2 network, where a larger mission link betweenness could cause more information flowing through a node or an edge during operational activities.

(2) Entropy of Mission link

$$E = -\sum_{c=1}^{N} I_c \ln I_c \tag{23}$$

where mission link entropy of C2 networks is denoted by E. Moreover, the significance of node v_c is denoted by I_c with the following definition,

$$I_c = \frac{b_c}{\sum_{c=1}^{N} b_c} \tag{24}$$

where b_c represents the mission link betweenness of the node v_c, and $\sum_{c=1}^{N} b_c$ captures the sum of the mission link betweenness among all nodes in C2 networks.

4. Simulation results

As shown in Fig. 1, a standard C2 network model was constructed to verify the rationality and validity of the two proposed invulnerability measures, which are for the mission link efficiency and mission link entropy. Subsequently, the sensing entity (C2 entity) and the fire strike entity can be indicated by nodes based on the theory of OODA cycle. Among these

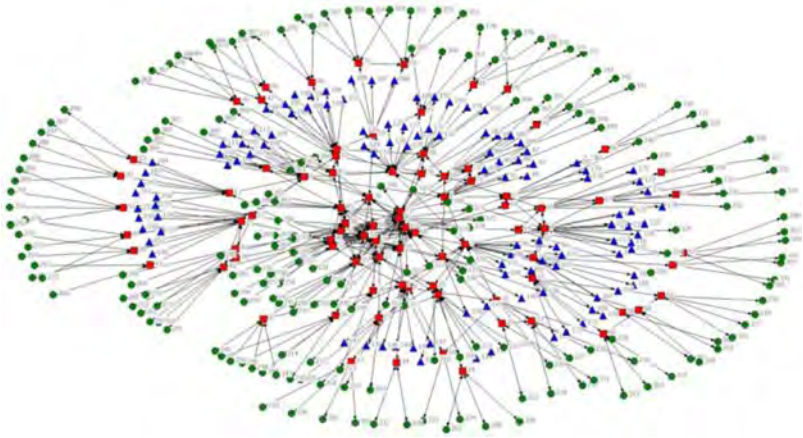

Fig. 1. C2 network model.

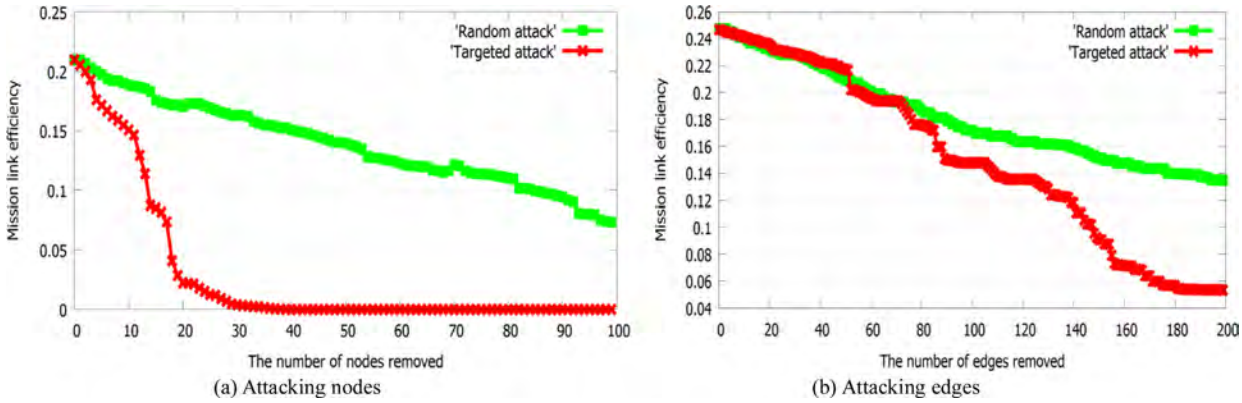

Fig. 2. The changing trend of mission link efficiency when nodes and edges are attacked.

nodes, all edges represent the interactive relationships of the entities. After implementing the Netdraw tool in the Ucinet social analysis software, a network model was automatically generated. In particular, the total number of nodes was N=391, the number of sensing nodes was n=107, the number of C2 nodes was t=85, and the number of fire strike nodes was m=199.

In general, there are two major consequences caused by network attacking. In particular, the efficiency of the network information transmission would be reduced, and the robustness of the network structure would be compromised [15]. In this paper, the network invulnerability was analyzed from the following two aspects, namely, the information transmission efficiency and the structural robustness [10]. On the one hand, the network efficiency and mission link efficiency were introduced to verify the measurements and comparisons of different information transmission efficiencies. On the other hand, several new concepts were also introduced to verify the measurements and comparisons of different structural robustness of the network structure. They included entropy of degree distribution [25], entropy of betweenness distribution [41], coefficient of network connectivity and entropy of mission link. Moreover, multiple simulations and comparisons were carried out in order to verify the validity of two measures, i.e. the mission link efficiency and mission link entropy.

4.1. Analysis of the invulnerability of C2 networks under different attacking strategies

C2 networks are often threatened by two common attacking strategies, which include random attacks and targeted attacks. In addition, the random attack refers to the attack on nodes (or edges) in C2 networks randomly with a certain probability; meanwhile, the targeted attack refers to the attack on nodes (or edges) in C2 network orderly with a certain strategy [26]. Therefore, both random attacking strategies and targeted attacking strategies were implemented in C2 networks in this paper. Furthermore, the invulnerability of networks was analyzed by changes in the C2 network's structure and performance, where the betweenness attack was the targeted attack [35]. The changing trend of mission link efficiency and mission link entropy when nodes and edges are attacked is shown in Figs. 2 and 3.

The comparative analysis of the changes in the efficiency and entropy of mission link was carried out for C2 network nodes and edges under different attacks. The results can be obtained and summarized as follows.

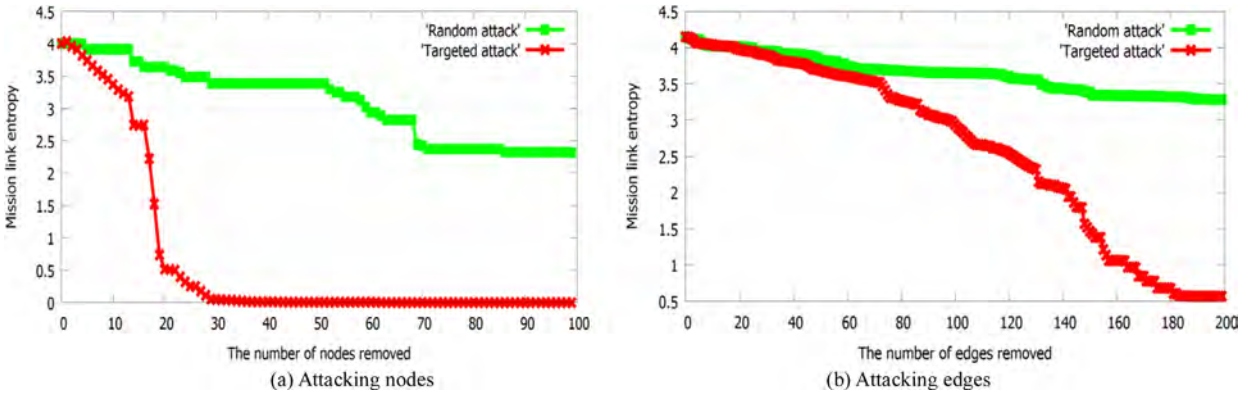

Fig. 3. The changing trend of mission link entropy when nodes and edges are attacked.

(1) The overall performance of the C2 network was deteriorated with the increasing node (or edge) failure ratio. Moreover, the mission link efficiency implied that the transmission rate of the C2 network was decreasing with the destruction of critical paths. On the other hand, the mission link entropy indicated the destruction of the C2 network structure with node or edge failures.
(2) Compared to edge failures, the node failures could significantly affect the network invulnerability. When nodes were under attacks, the efficiency and entropy of mission link mission link declined dramatically. In contrast, the efficiency and entropy of mission link mission link decreased in a relatively slow manner when edges were under attacks. Intuitively, this could be explained by the fact that the edges directly connected to a node would fail when a node was attacked.
(3) Compared with random attacks, targeted attacks on the C2 network were much more destructive, which illustrated the scale-free feature of C2 networks. In other words, the C2 network was very robust at random failures and fragile at targeted attacks. Therefore, it is necessary to protect the key nodes (or edges) in order to improve the network invulnerability.

In addition, to further verify the accuracy of measures, the mission link efficiency and mission link entropy was analyzed by comparisons with other measures in terms of the information transmission efficiency and structural robustness respectively. For example, under node attacks, multiple comparisons of changes in the network performance were carried out to analyze the invulnerability of C2 networks comprehensively. Various attacking strategies were applied in this work, which included the degree attacking strategy, the betweenness attacking strategy, the clustering coefficient attacking strategy and the mission link betweenness attacking strategy. It should be noted that all evaluation indexes were normalized before analyzing the performance of the network. The comparisons of different information transmission efficiencies are shown in Fig. 4.

Fig. 4 illustrated the changing trends of the network efficiency and mission link efficiency in terms of the information transmission efficiency. Under different attacking strategies, different network efficiencies and mission link efficiencies were obtained. Moreover, the following conclusions have been found according to Fig. 4.

(1) The overall decreasing rate of the mission link efficiency was higher than that of the network efficiency. That was because the mission link efficiency only captured the efficiency of the OODA loop, while the network efficiency was computing the information transmission rate via any link regardless of its validity. Thus, errors may occur during analyzing the invulnerability of C2 networks.
(2) Under random attacks, the mission link efficiency declined faster than the network efficiency; however, under targeted attacks, they decreased quite closely. Under random attacks, with the increasing proportion of sensing nodes and fire strike nodes, these nodes became less significant and therefore could not affect the network efficiency greatly. However, they could still break some original mission links, which significantly reduced the mission link efficiency. On the other hand, under targeted attacks, as C2 nodes were becoming more significant under targeted attacks, the C2 network was getting more vulnerable, which significantly affected both network efficiency and mission link efficiency. In conclusion, it was reasonable to use the mission link efficiency to measure the network invulnerability mission link, compared to the network efficiency. The comparisons of the structural robustness are shown in Fig. 5. The entropy of degree distribution of network can be calculated as follows [25]:

$$E = -\sum_{i=1}^{N} n_i \ln n_i$$

where n_i is the degree of node v_i, and E is the entropy of degree distribution of network G. Similarly, if n_i is the betweenness of node v_i, then E would be the entropy of betweenness distribution of network [41].

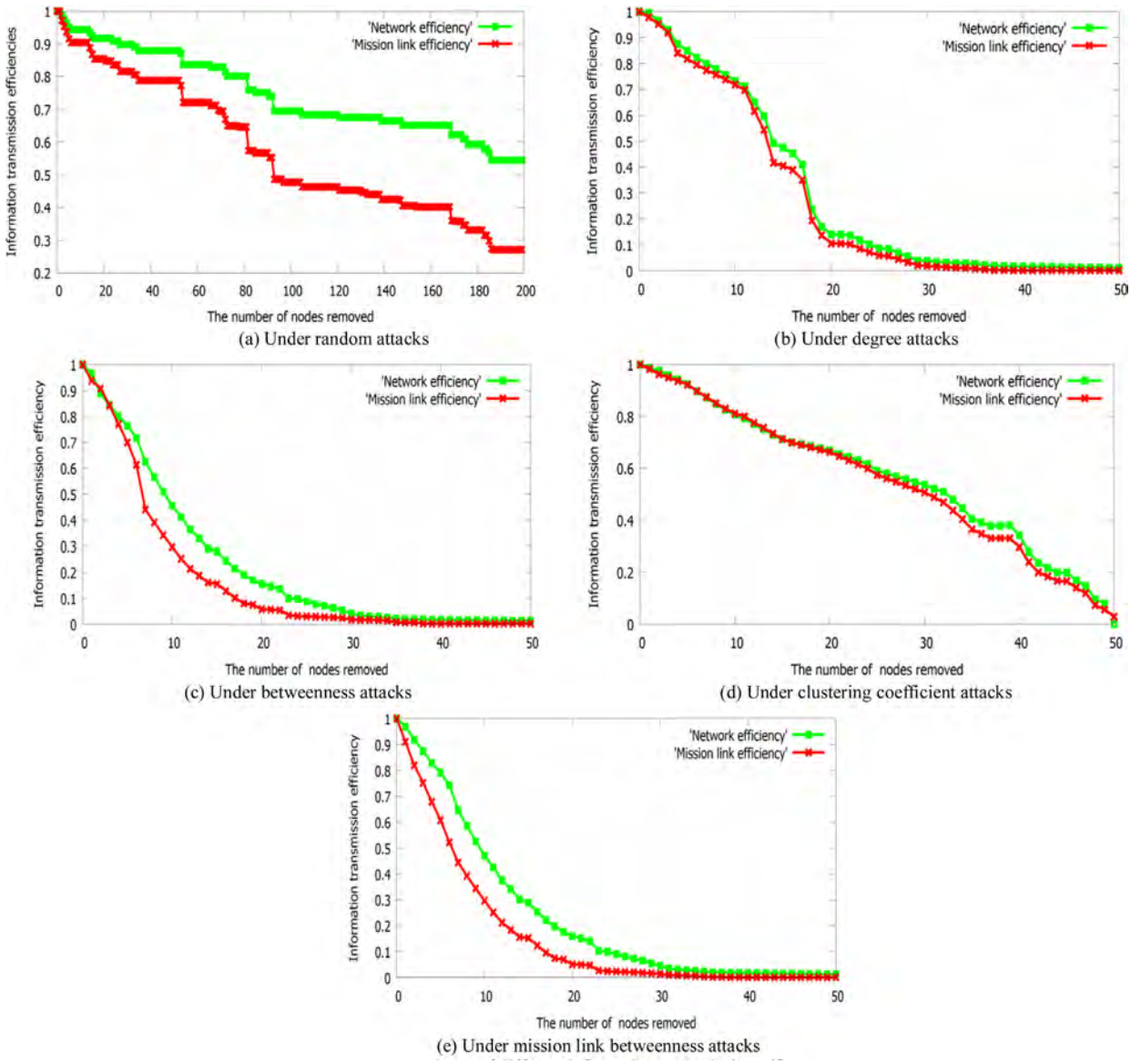

Fig. 4. Comparisons of different information transmission efficiencies.

In Fig. 5, the trend of common network robustness indexes with mission link entropy is presented. Moreover, the entropy of mission link was validated using multi measures with multiple attacking strategies. According to Fig. 5, the following conclusions can be found.

(1) Under random attacks, the network connectivity coefficient deviated from the other measurements. It was because of the defect of the connectivity coefficient itself. In other words, if there were more connected sub-graphs, the performance would be greatly compromised.
(2) Under targeted attacks, the most significant result was in degree distribution entropy. This could be explained by the fact that it was a local index and it was difficult to measure the overall structure of C2 networks.
(3) Under various attacking strategies, it could be observed that the mission link entropy was more stable and the evaluation results were less likely to volatile compared to the other structural robustness parameters. Furthermore, it was identical to the entropy of betweenness distribution, which can be seen from the above figures. In conclusion, the entropy of mission link entropy could evaluate the robustness of the C2 network structure in a more comprehensive and effective manner, since both global variable and combat function are considered.

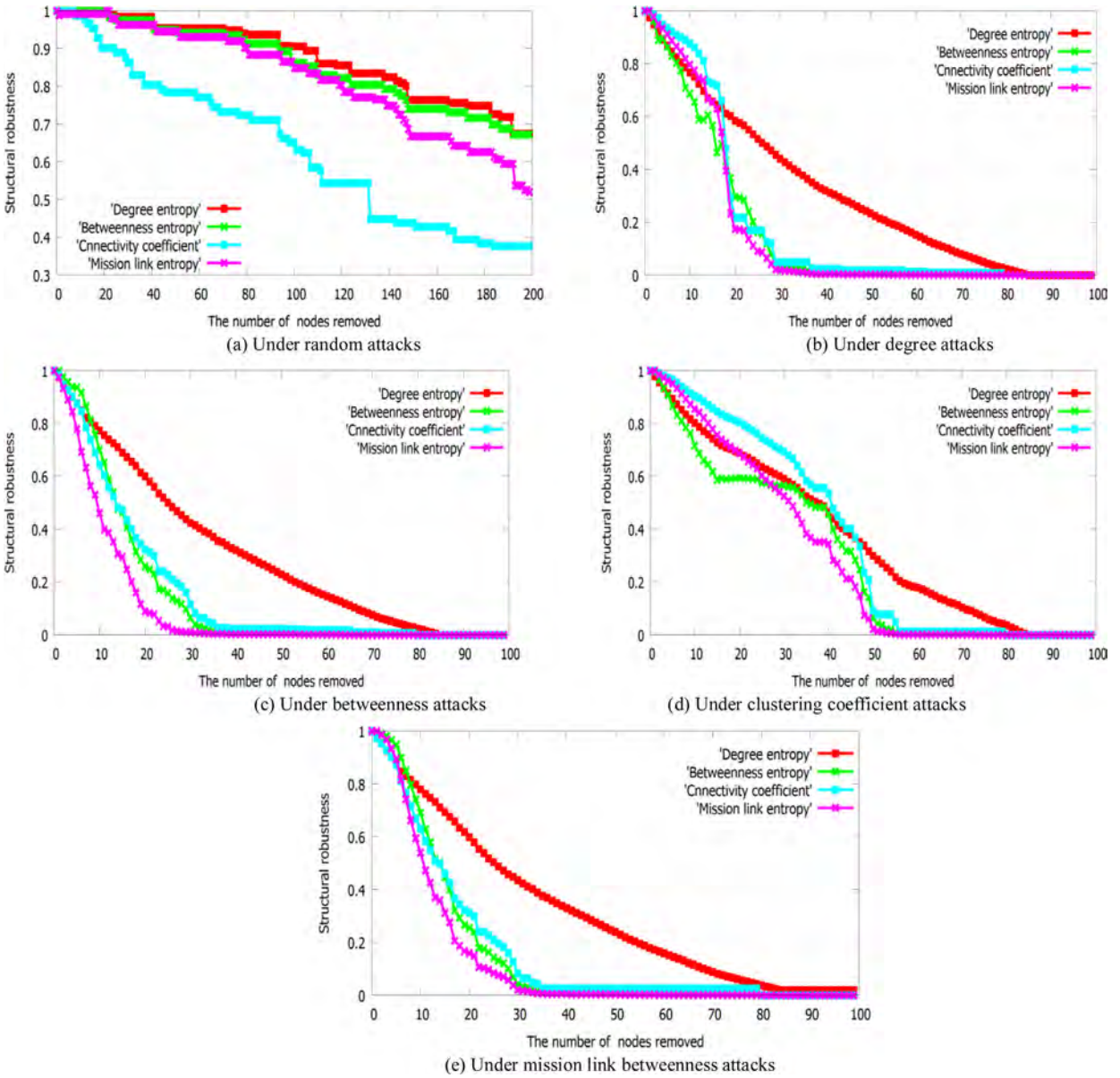

Fig. 5. Comparisons of the structural robustness.

4.2. Comprehensive analysis

It should be noted that nodes attacking and edges attacking are two extreme attacking types; therefore, the invulnerability of C2 networks might not be assessed comprehensively. During an actual combat, the node failures and edge failures are very likely to be mixed with a certain probability. Thus, it is rational to analyze the invulnerability of C2 networks with the assumption of mixed attacks on nodes and edges. For example, for targeted attacks, the invulnerability of the network when nodes and edges were under mixed attacks as indicated in Figs. 6 and 7.

After analyzing the changing trend of the network performance with nodes and edges under mixed attacks, the following conclusions have been obtained.

(1) It could be observed that both mission link efficiency and mission link entropy declined due to the mixed failures of nodes and edges.
(2) It is highly possible that the effect of mixed failures of nodes and edges on the network performance was not greater than that of only nodes' failures and only edges' failures. This result could be explained by the fact that the mixed

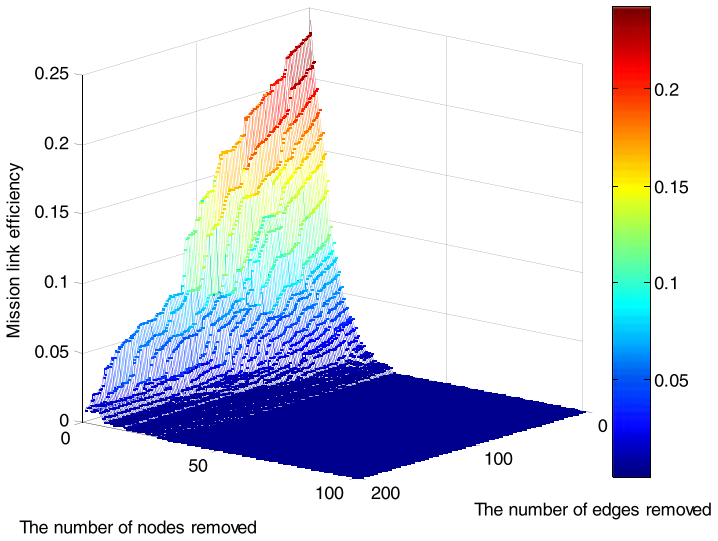

Fig. 6. Three-dimensional figure for mission link efficiency.

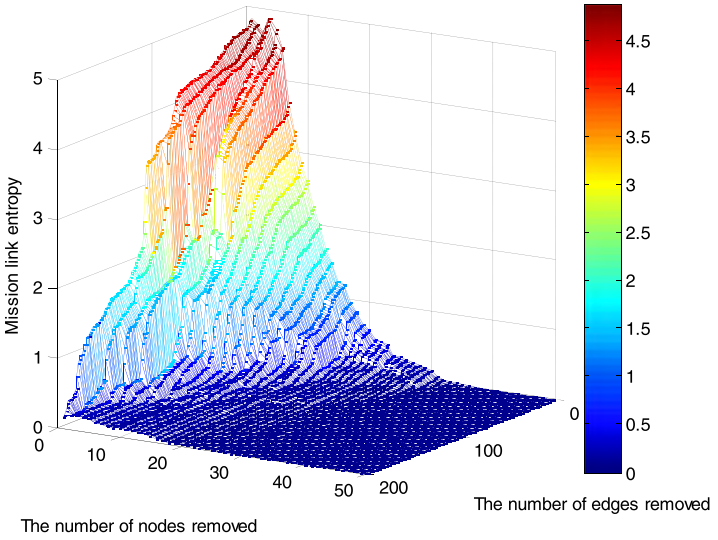

Fig. 7. Three-dimensional figure for mission link entropy.

failures included both nodes' and edges' failures, where nodes' failures affected the network performance much more significantly than edges' failures.

5. Conclusion

With the development of combat space and the enlargement of battle scopes, it is necessary for a large number of units to be merged into an integrated operational command-and-control network system. In fact, these types of networks have gradually become a fundamental operational organization with information technology. In this paper, a C2 network model was developed based on the super network, where the measures of invulnerability for C2 network were based on the efficiency and entropy of mission link. Furthermore, the invulnerability of C2 network was investigated in terms of the transmission efficiency and structural robustness, respectively. In particular, the simulation experimental results have indicated that the proposed measures are advantageous compared with the other traditional measures. Firstly, the proposed measures are more sensitive as well as accurate to evaluate the invulnerability of C2 networks. In addition, valuable references can be provided for the purpose of designing the C2 network with stronger invulnerability. However, there still exist various shortcomings in this work. Therefore, some possible future work is to focus on the dynamic evolution behavior of the C2 network and to perform analysis on the cascading invulnerability.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grants 91338104; the Defence Advance Research Foundation of China under Grants 61401310101 and 61400010301.

References

[1] D.S. Alberts, Agility quotient, in: Proceedings of 19th International Commamd and Control Research and Technology Symposium (ICCRTS), Washington DC, 2014.
[2] R. Albert, H. Jeong, A.L. Barabas, Error and attack tolerance of complex networks, Nature 406 (2000) 378–382.
[3] Q. Bian, T. Hang, L. Hui, M. Fang, Research on the diameter and average diameter of undirected double-loop networks, Ninth International Conference on Grid and Cloud Computing, Nanjing, 2010.
[4] A.L. Barabasi, R. Albert, Emergence of scaling in random networks, Science 286 (5439) (1999) 509–512.
[5] J.R. Cares, A Incorporated, An information age combat model, 9th International Command and Control Research and Technology Symposium, Copenhagen, Denmark, 2004.
[6] C. Deng, The robustness analysis of wireless sensor networks under uncertain interference, Sci. World J. 2013 (2013) 185970.
[7] S. Deller, M.I. Bell, S.R. Bowling, G.A. Rabadi, A. Tolk, Applying the information age combat model: quantitative analysis of network centric operations, Int. C2 J. 3 (01) (2009) 1–25.
[8] S. Deller, G. Rabadi, A. Tolk, S.R. Bowling, Organizing for improved effectiveness in networked operations, Operat. Res. Unmanned Syst. 17 (01) (2012) e45681.
[9] T. Enokido, M. Takizawa, Purpose-based information flow control for cyber engineering, IEEE Trans. Ind. Electron. 58 (06) (2011) 2216–2225.
[10] W. Fan, S. Huang, S. Mei, Invulnerability of power grids based on maximum flow theory, Physica A 462 (2016) 977–985.
[11] N. Ghazisaidi, M. Scheutzow, M. Maier, Survivability analysis of next-generation passive optical networks and fiber-wireless access networks, IEEE Trans. Reliab. 60 (02) (2011) 479–492.
[12] X. He, Y. Wu, Affects of production adjustment strategy between manufactures on supply chain stability, Sci. Technol. Manage. Res. 32 (21) (2012) 225–228.
[13] X. Hu, X. He, D. Rao, A methodology for investigating the capabilities of command and coordination for system of systems operation based on complex network theory, J. Complex Syst. Complexity Sci. 12 (02) (2015) 9–17.
[14] F. Hu, H. Zhao, J. He, F. Li, S. Li, Z. Zhang, An evolving model for hypergraph-structure-based scientific collaboration networks, Acta Physica Sinica 62 (19) (2013) 198901.
[15] Y. Hao, J. Han, Y. Lin, L. Liu, Vulnerability of complex networks under three-level-tree attacks, Physica A 462 (2016) 674–683.
[16] Z. Jiang, M. Liang, D. Guo, Enhancing network performance by edge addition, Int. J. Modern Phys. C 22 (11) (2012) 1211–1226.
[17] W. Lu, S. Liu, Y. Yang, Design for the emergency command information system architecture of ocean oil spill, Aquatic Procedia 03 (2015) 41–49.
[18] O. Lordan, J.M. Sallan, P. Simo, D. Gonzalez-Prieto, Robustness of airline alliance route networks, Commun. Nonlinear Sci. Numer. Simul. 22 (01) (2016) 587–595.
[19] Y. Lan, K. Deng, S. Mao, H. Wang, K. Yi, M. Lei, Adaptive evolvement of information age c4isr structure, J. Syst. Eng. Electron. 26 (02) (2015) 301–316.
[20] P. Liu, F. Liao, H. Huang, H. Timmermans, Dynamic activity-travel assignment in multi-state supernetworks under transport and location capacity constraints, Transportmetrica A 12 (07) (2016) 572–590.
[21] Y. Lan, H. Wang, K. Yi, S. Mao, "Five-loop" model and its effectiveness representation for network-centric C4ISR system structure, J. Syst. Eng. Electron. 37 (01) (2015) 93–100.
[22] D. Li, Y. Jiang, R. Kang, S. Havin, Spatial correlation analysis of cascading failures: congestions and blackouts, Sci. Rep. 4 (2014) 5381.
[23] Z. Lu, X. Li, Attack vulnerability of network controllability, Plos One 11 (09) (2016) e0162289.
[24] L. Lü, D. Chen, X. Ren, Q. Zhang, Y. Zhang, T. Zhou, Vital nodes identification in complex networks, Phys. Rep. 650 (2016) 1–63.
[25] P. Luo, Y. Li, C. Wu, Complex networks evolution research using the network structure entropy, Complex Syst. Complexity Sci. 10 (04) (2013) 62–68.
[26] T. Nie, Z. Guo, K. Zhao, Z. Lu, The dynamic correlation between degree and betweenness of complex network under attack, Physica A 457 (2016) 129–137.
[27] J. Peng, J. Xiong, G. Xu, Analysis of diffusion and trapping efficiency for random walks on non-fractal scale-free trees, Physica A 407 (2014) 231–244.
[28] X. Song, W. Shi, G. Tan, Y. Ma, Multi-level tolerance opinion dynamics in military command and control networks, Physica A 437 (2015) 322–332.
[29] Z. Su, L. Li, H. Peng, J. Kurths, J. Xiao, Y. Yang, Robustness of interrelated traffic networks to cascading failures, Sci. Rep. 4 (2014) 1–7.
[30] F. Shao, R. Sun, S. Li, Y. Sui, Research of multi-subnet composited complex network and its operation, Complex Syst. Complexity Sci. 9 (04) (2012) 20–25.
[31] D. Shizuka, D.R. Farine, Measuring the robustness of network community structure using assortativity, Animal Behav. 112 (2016) 237–246.
[32] I. Wu, H. Deng, Y. Tan, Spectral measure of robustness for internet topology, 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), 2010.
[33] X. Wang, J. Cao, X. Qin, Study of robustness in functionally identical coupled networks against cascading failures, PLOS ONE 11 (08) (2016) e0160545.
[34] D.J. Watts, S.H. Strogatz, Collective dynamics of small-world networks, Nature 393 (6684) (1998) 440–442.
[35] S. Wang, J. Liu, Robustness of single and interdependent scale-free interaction networks with various parameters, Physica A 460 (2016) 139–151.
[36] C. Yen, M.Y. Yeh, M. Chen, An efficient approach to updating closeness centrality and average path length in dynamic networks, IEEE 13st International Conference on Data Mining, Dallas, TX, 2013.
[37] X. Yu, S. Wang, Measuring the network efficiency and the component importance for multiclass transportation network, 2th International Conference on Information Science and Control Engineering (ICISCE), Shanghai, 2015.
[38] H. Zhang, N. Huang, H. Liu, Network performance reliability evaluation based on network reduction, in: Proceedings of Reliability and Maintainability Symposium, Colordao Springs, CO, 2014.
[39] J. Zhang, Y. Lan, K. Yi, S. Mao, H. Wang, Model and solving method for adaptive evolution of command and control relationship in C4ISR system, J. Syst. Eng. Electron. 37 (07) (2015) 1543–1550.
[40] F. Zhang, Entropy optimization of scale-free networks robustness to targeted attack, Inf. Technol. J. 12 (09) (2013) 1868–1872.
[41] Q. Zhang, X. Lu, M. Li, Y. Deng, S. Mahadevan, A new structure entropy of complex networks based on nonextensive statistical mechanics, Int. J. Modern Phys. C 27 (10) (2016) 440–462.