IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 18, 2017, accepted October 21, 2017, date of publication November 3, 2017, date of current version March 9, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2769964

Invulnerability Measure of a Military Heterogeneous Network Based on Network Structure Entropy

XIUE GAO[1,2], **KEQIU LI**[1], **(Senior Member, IEEE), AND BO CHEN**[2]
[1]School of Computer Science and Technology, Dalian University of Technology, Dalian 116024, China
[2]School of Information and Engineering, Dalian University, Dalian 116622, China

Corresponding author: Bo Chen (chenbo20040607@126.com)

This work was supported by the National Natural Science Foundation of China under Grant 61571074, Grant 61540024, Grant 61540023, Grant 91338104, and Grant 61301151.

ABSTRACT Military heterogeneous networks often suffer from node or edge failures due to attacks, which lead to whole network topology segmentation or even paralysis. Therefore, structural invulnerability is the major technical bottleneck that impedes the combat capability of military heterogeneous system. Nodes are mainly considered in current methods, with little attention paid to edges. As such, current methods cannot accurately evaluate the structural invulnerability of military heterogeneous networks. This paper presents a new method of evaluating the survivability of military heterogeneous networks, based on network structure entropy. A model of survivability is proposed based on the network irreversibility which considers not only the nodes but also the edges. The node criticality is calculated by the level flow betweenness. Edge criticality is put forward based on the edge correlation factor and information transmission efficiency. Simulation results show that this invulnerability measure has the characteristics of high sensitivity and high precision, which will provide a theoretical basis for designing and optimizing the structure of the military heterogeneous network.

INDEX TERMS Complex network, invulnerability measure, military heterogeneous network, structure entropy.

I. INTRODUCTION

Maintaining the stability of modern infrastructures such as power systems, traffic networks, financial systems, military heterogeneous networks, and protecting them from failures (random failures or intentional attacks) is an active topic of research in the study of network security [1]. A military heterogeneous network is the carrier of modern warfare information transmissions and the basis of integrated joint operations as well as the basic networks that ensure interconnection, intercommunication and interoperability between each system [2]. A military heterogeneous network is the basis of seizing information superiority, which is converted into decision superiority and battle operation superiority in information warfare. A military heterogeneous network is not only the link to connect the early warning detection systems with the command and control systems, and firepower systems, etc., but is also important in guaranteeing that the operational elements provide a full and synchronized operations [3]. Therefore, the key nodes and links of the military heterogeneous network become the focus of attacks on both sides [4]. Military heterogeneous networks often suffer from node or edge failures due to attacks, which cause the topology partition or paralysis of the entire network [5]. The high invulnerability of a military heterogeneous network is the basic premise to improve the combat capability of the integrated joint operational command system [6] as well as the efficient evaluation of the entire combat efficiency and ability to complete the combat mission. Currently, researchers carry out research primarily on structure modeling and network robustness in the field of military heterogeneous network based on complex network theory and super network theory. In particular, the robustness of the network is mainly studied from the aspects of anti-survivability and invulnerability measurement. Further analysis shows that static invulnerability and cascading failure [7], [8] are the two main directions of network invulnerability research. However, in terms of invulnerability measures, there is no suitable measurement to measure the invulnerability of military heterogeneous network. Therefore, the invulnerability of military heterogeneous networks has become a research hotspot [9], [10].

Initial research focused on the invulnerability of complex networks included work by Albert, who proposed an invulnerability measure index based on the maximum connected subgraph and average path length [11]. At present, graph theory, complex network theory and super network theory are the main basic theories used to study network invulnerability. The research is primarily devoted to their influence on the topology and network performance. However, in the field of nonlinear control theory, such as adaptive fuzzy control [12], [13], adaptive intelligent control [14], and adaptive neural tracking control [15], the research core of system robustness is the influence of external factors such as time delay and input saturation on system stability, rapidity and accuracy. Therefore, some mature control theories cannot be used directly in the research of network invulnerability. Subsequently, many scholars began to research the evaluation methods of network invulnerability. This is mainly from several aspects of research, such as the network connectivity, network efficiency, node criticality and network dynamic evolution [16].

On the topic of network connectivity, Ming [17] proposed the Network Recovery Degree (NRD) as the measure of complex network invulnerability; abstracted the connectivity of nodes, service quality and connection degree; and defined the concept of Source-Destination Pair (SD Pair), which reflects the overall network performance. Wu [18], [19] established the theory of the spectral measure for complex network invulnerability and proposed a natural connectivity index; this measure calculated the weighted sums of different lengths of the closed loop, which described the redundancy of alternatives in the network. Wu [20] proposed the invulnerability measure of natural connectivity, which establishes the relationship between the spectral characteristics and invulnerability of the complex network. Ernestro et al. [21], [22] further researched the natural connectivity and local natural connectivity of the weighted network. Wang [23] defined the estimation rule of the network distance based on the characteristics of a large-scale network, which proposed an invulnerability measure based on the subsystem failure distance and entropy theory. This approach is applicable to the large-scale network, and the algorithm is simple but imprecise. Rak [24] researched the invulnerability problem of regional failure for a Wireless Mesh Network (WMN), which proposed three applicable invulnerability quantitative evaluation methods, including the Regional Failure invulnerability Function (RFS), p-partition invulnerability function and expected total flow ratio as well as performing simulation and analysis of these three evaluation methods. Li and Dekker [25], [26] proposed the use of the Perron-Frobenius characteristic value (PFE) for the Information Age Combat Model (IACM) network adjacency matrix to measure the network performance, but the author did not introduce the specific application methods of IACM, validity of PFE and other problems by theoretical derivation or experimental verification. Deller [27], [28] performed further research based on Cares's IACM theoretical model, and simulation was performed based on Netlogo. This study preliminarily verified the rationality of PFE as an evaluation index of the network operational effectiveness, but the simulation experiments had significant limitations, including: the decision nodes were not connected to the network, network scale was too small, and the difference of the node's own ability was not considered.

The evaluation indexes based on the network efficiency include the network diameter, average diameter, average path length and network efficiency. Bian [29] proposed an efficient algorithm for calculating the average diameter of a directed double loop network when researching the minimum path graphs of double loop networks, and then simulated the relationship between the network and average diameters. The study found that the average diameter is better than the network diameter to measure the efficiency of network transmission. Yen [30] put forward CENDY, a kind of algorithm for network transmission efficiency, which can quickly calculate the betweenness centrality and average path length of a dynamic network. Wang [31] presented a new measure of survivability, which is characterized by strong versatility and scalability, and the new measure can be applied to many network models. However, the algorithm complexity of this method was high. Considering multiple failures, the connection state of the mobile terminal and the continuous Markov chain are considered. Peng [32] proposed an evaluation model for survivability of Mobile Ad-hoc Networks (MANETs). Ming [33] proposed new index architecture with 24 indicators based on the protection-detection-response (PDR) security model and R3 invulnerability rules, which can fully reflect the invulnerability and apply to a variety of network models. Due to the problem of the algorithm complexity, this index architecture was not applicable to a large scale network. Yu [34] redefines the network efficiency to measure the efficiency of information transmission for the multi class network, which uses time-based decision criterion (TBDC) and monetary-based decision criterion (MBDC) standards to measure the rationality of this index. The study shows that this index is very effective.

In the aspect of node criticality, Dekker [35] used the edge weight to measure key nodes in the large-scale complex network, proposed an evaluation model of the network invulnerability measure and the network invulnerability obtained by calculating the node invulnerability. Yang [36] proposed an invulnerability evaluation index matrix for an instant messaging network, which provided an instant messaging network invulnerability influence factor and the evaluation index, determined by the entropy method.

In terms of network dynamic evolution, Hwang [37] proposed invulnerability evaluation methods aimed at both dynamic and static combat systems, integrated the Discrete Event Simulation Specification(DEVS) form theory, System Equity Structure/Model Base (SES/MB) framework and agent technology, which has strong relevance.

Khalid [38] proposed a quantified invulnerability evaluation model, which applied the time that the network switches to a normal working state under attack. And it conducted invulnerability analysis on the unreliable multi service queue with the processes of "arrive, services, fault and maintenance". Sazia [39] proposed two kinds of DEVS invulnerability evaluation models based on soft recovery with reconstruction and key revocation, verifying the feasibility of the two models at the same time.

The invulnerability measure not only reflects the ability of the infrastructure network to resist attacks, but also evaluates the hazards caused by infectious diseases, rumors or viruses, and it is of great significance to evaluate the robustness of the network. Nevertheless, the invulnerability measures described above consider only the nodes, not edges, which cannot accurately evaluate the structure invulnerability of the military heterogeneous network. Inspired by the above discussion, in this paper, a new invulnerability measure is proposed for military heterogeneous network based on network structure entropy. Compared with the existing results, the main contributions of this paper are concluded as follows:

- In this paper, a new method to evaluate the invulnerability of military heterogeneous networks based on network structure entropy is proposed.
- A model of survivability that considers both the nodes and the edges, is proposed based on the network irreversibility. In particularly, the node criticality is calculated by the level flow betweenness, and edge criticality is defined based on edge association factor and information transmission efficiency.
- Simulation, and the comparison with existing related results are provided to verify the rationality and effectiveness of the metrics proposed by this paper.
- The invulnerability measurement proposed by this paper would better reflect the network invulnerability against both failure and attack, and it provides a theoretical basis for designing and optimizing the structure of the military heterogeneous network.

The rest of this paper is organized as follows: In Section II, we propose node criticality based on the Level Flow Betweenness (LFB) and, edge criticality based on edge correlation factors combined with information transfer efficiency. Section III establishes a model of structure entropy based on network invulnerability and provides its procedure algorithm. Experimental validation, analysis of the effectiveness and practicability of this invulnerability measure are given in Section IV. Section V is devoted to conclusion and future research direction.

II. NETWORK INVULNERABILITY

According to the combat theory of Orient – Observe – Decide – Act (OODA), the combat processes of the Command and Control systems are as follows: observe node collection and converge the situation information to intelligence processing nodes. These nodes distribute information after data fusion and processing to command nodes of all kinds and at all levels, giving commanding orders to fire a strike node after cooperation and decision, providing battle effectiveness. The ability of information processing and transmission for the military heterogeneous network is an important protection to improve the system combat capability. At the same time, nodes and links in the network guarantee the reliable operation of the system. Therefore, both nodes and edges need to be considered for the evaluation of survivability in military heterogeneous network.

A. NODE CRITICALITY

As a huge and complex system, the military heterogeneous network not only has the typical characteristics of a complex network, it also has peculiar characteristics of structure hierarchy, load non-uniformity and more. An undirected network graph *G=(V,E)* can describe the military heterogeneous network structure, where V represents the node collections and E represents the edge collections. The number of nodes is N, and the number of edges is m. $A = [a_{ij}]$ is the adjacency matrix of G, the element $a_{ij} = 1$, when there is an edge between node i and node j, otherwise, $a_{ij} = 0$.

The initial information of all nodes in the military heterogeneous network is 1 ($H(v_j) = 1$), and only one node sends information at a time, other nodes receive information. During the information walk through the military heterogeneous network, if the degree of the node v_j is k_j and the information content is $H(v_j)$, the information content for nodes, which are connected to node v_j, directly receives $H(v_j)/k_j$. In order to make sure that the total content of information is a fixed value, the value is returned to 0 after the node's message is sent out. The Level Flow Betweenness in military heterogeneous network can be obtained, as:

$$H_n(v_i) = \sum_{j=1}^{N} \frac{H_{n-1}(v_j)}{k_j} \cdot a_{ij} \tag{1}$$

where k_j is the degree of node v_j and $H_{\mathrm{n}-1}(v_j)$ is the amount of information after an iteration. n is the iteration time, which is not larger than the military heterogeneous levels.

Assuming that the adjacency matrix A of military heterogeneous network is as follows:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1N} \\ a_{21} & a_{22} & \cdots & a_{2N} \\ \vdots & \vdots & & \vdots \\ a_{N1} & a_{N2} & \cdots & a_{NN} \end{pmatrix}$$

It can be seen from the algorithm description, the information random walk for each time period requires $N - 1$ iterations. During the first time of the information random walk, it randomly selects the node v_j as the start node in the first iteration and searches for the nodes that are directly connected to node v_j from other $N - 1$ nodes. The algorithm complexity of this step is as follows:

$$f_1 = o(N - 1)$$

TABLE 1. Algorithm complexity chart.

Algorithm	Complexity
EIG	$o(N^4)$
BET	$o(N^3)$
AFB	$o(dia \times N^2)$
LFB	$o(D \times N^2)$

Similarly, the algorithm complexity of the second iteration is also approximately $f_2 = o(N-1)$; in the same way, the complexity of the *Nth* iteration is $f_N = o(N-1)$.

Thus, the algorithm complexity of one step is:

$$F = f_1 \cdot f_2 \cdot \cdots \cdot f_N$$

After the D information random walk, the entire algorithm complexity of the key nodes identification is as follows:

$$\begin{aligned} F' &= DF = D(f_1 \cdot f_2 \cdot \cdots \cdot f_N) \\ &= D(o(N-1) \cdot o(N-1) \cdot \cdots \cdot o(N-1)) \\ &= o(D(N-1)N) = o(DN^2 - DN) \approx o(DN^2) \end{aligned} \tag{2}$$

The complexity of the eigenvector (EIG) in the common matrix is almost close to $o(N^4)$, algorithm complexity of betweenness (BET) is about $o(N^3)$, and complexity of the approximation flow betweenness (AFB) is about $o(dia \times N^2)$. The algorithm complexity of the LFB is proposed in this paper as $o(D \times N^2)$. The complexity comparisons of these four methods are shown in Table 1.

Level flow betweenness takes into account the characteristics of military heterogeneous network topologies (global superiority) and network information walk paths (local superiority), which reduces the complexity of the algorithm and becomes increasingly precise. Level flow betweenness can precisely describe node criticality. The definition of node criticality in the military heterogeneous network is as follows:

$$CV(v_i) = H_n(v_i) \tag{3}$$

B. EDGE CRITICALITY

The edge of military heterogeneous network is the path to connect the two nodes, which plays an important role in the structure and properties of military heterogeneous network. The communication of the two nodes will be interrupted if the edge is attacked, which makes the network performance decline and even results in paralysis of the global network. Accordingly, the invulnerability evaluation of the military heterogeneous network needs to consider the criticality of the network edge. The edge is affected by many factors in military heterogeneous networks, the edge correlation factor and information transmission efficiency is the most important factors. Therefore, the quantitative results of the correlation factor and information transmission efficiency can describe the edge criticality.

1) EDGE CORRELATION FACTOR

The edge correlation factor is defined as the degree of influence of a certain edge by its two endpoints. The bigger the node criticality is, the greater the influence on its edge is. At the same time, with increasing command and control flow distributed by nodes, the criticality of the edge is increased. Thus, the edge correlation factor is obtained by quantifying the influence coefficient of nodes. The edge correlation factor between nodes v_i and v_j is as follows:

$$\eta_{ij} = \frac{\max(CV(v_i), CV(v_j))}{CV(v_i) + CV(v_j)} \tag{4}$$

2) INFORMATION TRANSMISSION EFFICIENCY

The edge properties of military heterogeneous networks include the transmission distance and link bandwidth. This paper constructs the coefficient matrix $L_E = [l_{ij}]_{N \times N}$ between nodes as the transmission efficiency, where l_{ij} satisfies:

$$l_{ij} = \begin{cases} \frac{1}{d_{ij}}, & i \neq j \\ 1, & i = j \end{cases}$$

d_{ij} is the space distance between nodes v_i and v_j.

The average transmission efficiency I_i of any node v_i can be calculated through l_{ij} as follows:

$$I_i = \frac{2}{N(N-1)} \sum_{j=1, j\neq i}^{N} l_{ij} = \frac{2}{N(N-1)} \sum_{j=1, j\neq i}^{N} \frac{1}{d_{ij}} \tag{5}$$

This equation describes the transmission efficiency of the node in a military heterogeneous network.

3) EDGE CRITICALITY

Combined with the edge correlation factor and information transmission efficiency, the edge criticality matrix $W = [w_{ij}]_{N \times N}$ is defined as:

$$W = \left\{ \begin{matrix} I_1 & a_{12}I_1\eta_{12} & \cdots & a_{1N}I_1\eta_{1N} \\ a_{21}I_2\eta_{12} & I_2 & \cdots & a_{2N}I_2\eta_{2N} \\ \vdots & \vdots & \vdots & \vdots \\ a_{N1}I_N\eta_{N1} & \cdots & \cdots & I_N \end{matrix} \right\} \tag{6}$$

where $w_{ij} = a_{ij}I_i\eta_{ij}$ is the edge criticality between nodes v_i and v_j, a_{ij} is the element of the adjacency matrix A. For convenience of expression, set $CE(e_{ij}) = w_{ij} = a_{ij}I_i\eta_{ij}$.

III. INVULNERABILITY MEASURE BASED ON NETWORK STRUCTURE ENTROPY

A. CRITICAL COEFFICIENT OF NETWORK

We consider both the node and edge criticality when measuring the criticality of the military heterogeneous network. The comprehensive critical degree of the node is defined as $CS(v_i)$:

$$CS(v_i) = \gamma \cdot CV(v_i) + \mu \cdot \frac{1}{|S|} \sum_{j \in S} CE(e_{ij}) \tag{7}$$

where γ and μ are the weights of the node and edge criticality, $\gamma + \mu = 1$. S is a set of nodes that are directly connected to the node v_i.

The critical coefficient of node v_i in the military heterogeneous network is defined as S_i:

$$S_i = CS(v_i) / \sum_{i=1}^{N} CS(v_i) \tag{8}$$

B. MODEL OF NETWORK STRUCTURE ENTROPY

Entropy is a uniformity measure of the network. Rudolf first proposed this concept in 1950 [40]. Entropy was originally used in thermodynamics. The more uniform the energy distribution of the system is, the greater the entropy value is. By analogy, the distribution of this key coefficient of the network node reflects the invulnerability of networks when they suffer attack. The more uniform the critical coefficient distribution is, the stronger the invulnerability of the military heterogeneous network is. The network structure entropy is calculated as:

$$E = -\sum_{i=1}^{n} S_i In S_i \tag{9}$$

C. ALGORITHM REALIZATION

The detailed process steps of the invulnerability measure model based on network structure entropy are as follows:

Step 1: Calculate node criticality. According to the structural characteristics of a military heterogeneous network, and considering both global and local information, the criticality $CV(v_i)$ of each node is calculated. $CV(v_i)$ is equal to the level flow betweenness of node v_i on the numerical value.

Step 2: Calculate edge criticality. The edge critical matrix is set up by computing the two factors that influence the edge criticality, yielding the criticality $CE(e_{ij})$ of all edges in the military heterogeneous network, with e_{ij} being the edge between nodes v_i and v_j.

Step 3: Calculate the critical coefficient S_i of network. The criticality of nodes and edges in a military heterogeneous network is obtained, which maps to the node comprehensive criticality $CS(v_i)$. The critical coefficient S_i of the network is then calculated.

Step 4: Calculate the network structure entropy. This paper uses the critical coefficient S_i of the network to calculate the network structure entropy

IV. SIMULATION AND ANALYSIS

To verify the rationality and effectiveness of the invulnerability measurement for the military heterogeneous network based on the network structure entropy, a typical military heterogeneous network model is shown in FIGURE 1. The command entities are abstracted into nodes and relationships between entities are abstracted into edges. Additionally, different edges represent different links, which include command and cooperative relationships. Among the relationships, the command relationship consists of the step-level and leapfrog-level command. A cooperative relationship consists of internal and external cooperations. The number of nodes is $N = 453$ in the military heterogeneous network model, which includes 85 military heterogeneous nodes, 256 fire nodes and 112 sensing nodes. The command level is 4. As shown in FIGURE 1, the red circles in the topology represent a military heterogeneous node, blue square represents a fire node, and black triangles, the sensing nodes. This paper uses random and deliberate attack strategies to verify the network invulnerability.

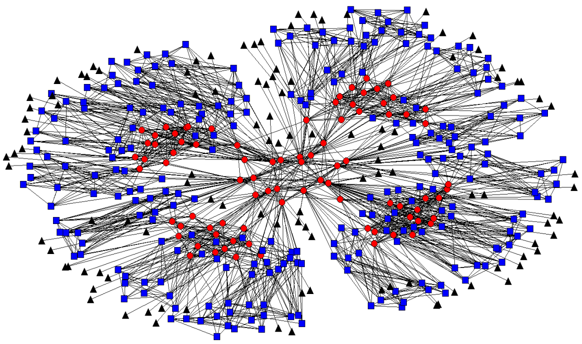


FIGURE 1. Military heterogeneous network model.

With random attacks, the changes of the node structure entropy and edge structure entropy are shown as in FIGURE 2.

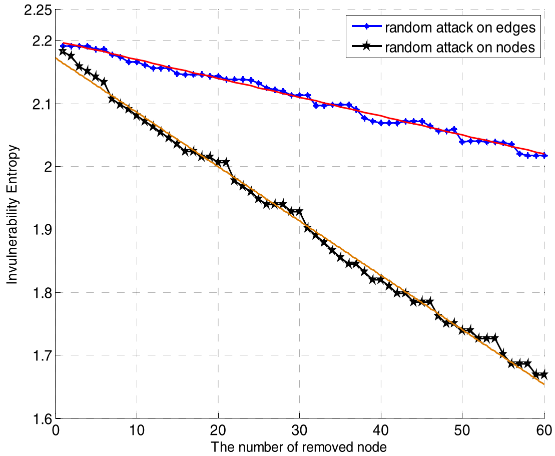


FIGURE 2. The changes of the node and edge structure entropy under random attack.

As shown in FIGURE 2, the changes of structure entropy are different when the node and edge are attacked randomly in a military heterogeneous network. The structure entropy rapidly declines when the node is attacked. By contrast, the structure entropy decreases relatively gently when the edges suffer attack. In other words, the military heterogeneous network appears more vulnerable under node-based attack than under edge-based attack, which implies that the node-targeted attack is more destructive than the edge-targeted attack. This finding is consistent with the results of current studies [7]. When the nodes are attacked, the edges directly connected with them will also be affected. Therefore, the nodes are more important than the edges in the military heterogeneous network. When assigning the parameters γ and μ in the structure entropy of a military heterogeneous network, we need to notice that the weight of node criticality is bigger than the edge. Two curves fit into one straight line in FIGURE 2.

The fitting straight slopes of node k_n and edge k_e are calculated when nodes or edges are under random attack. The solution formula of λ and μ is calculated as follows:

$$\frac{\lambda}{\mu} = \frac{k_n}{k_e} \approx \frac{3}{1} \tag{10}$$

Based on $\lambda + \mu = 1$, the weight of the node criticality is $\lambda = 0.75$ and weight of the edge criticality is $\mu = 0.25$.

The result of the network structure entropy is shown in FIGURE 3 when the military heterogeneous network is under random and deliberate attack. The deliberate attack contains a variety of attacks, including the random, degree-rank, approach degree-rank, eigenvector-rank, betweenness-rank, and approximate flow betweenness-rank attacks.

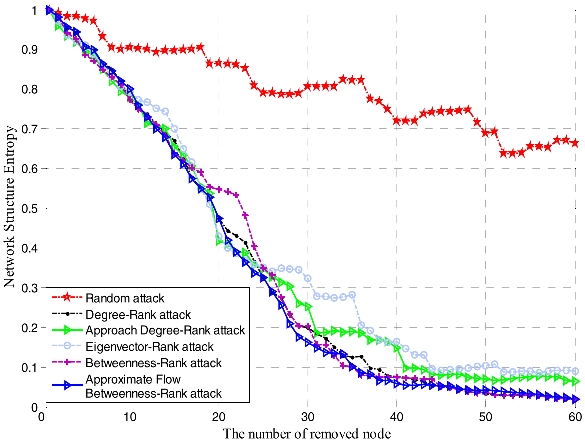


FIGURE 3. The effect of network structure entropy by different attacks.

As shown in FIGURE 3, the network structure entropy decreases slowly when the military heterogeneous network suffers random failure. However, the network structure entropy drops swiftly when the network suffers deliberate attack. From FIGURE 3, we can learn that the network structure entropy is still greater than 0.7 after 50 nodes are removed randomly; there is little damage to network. However, when 20 nodes are deliberately deleted, the network structure entropy is less than 0.5, leading to the network communication capabilities becoming very poor. In particular, the network structure entropy is even less than 0.2 when 40 nodes are deliberately attacked, which leads to poor network connectivity and many isolated nodes. The results show that the military heterogeneous network is matched with the scale-free characteristics of a complex network. This is to say, the military heterogeneous network is much more robust to random attack but extremely fragile to deliberate attack.

To verify the effectiveness and rationality of the proposed invulnerability measure, this study compares the network structure entropy with the network average efficiency, the network connectivity coefficient and the network natural connectivity. For the convenience of analysis, all the survivability measures are normalized.

The average efficiency η is the sum of an inverse distance of any node pairs [24]. η is calculated as:

$$\eta = \frac{2}{N(N-1)} \sum_{i \neq j} \frac{1}{d_{ij}} \tag{11}$$

Obviously, $\eta \in [0, 1]$, when there are no connecting paths linking any nodes, $\eta = 0$; and when the network is a complete graph, $\eta = 1$. η stands for the transmission capability of information flow in the network. The network average efficiency measures the invulnerability of the military heterogeneous network from the information transmission path perspective. After a military heterogeneous attack, the efficiency is higher, while there is better network survivability.

The relationship of the survivability and component number of subgraphs is reflected by the network connectivity coefficient. It is defined as follows [41, 42]:

$$C = \frac{1}{2^{w}\frac{N_i}{N}\sum_{i=1}^{\omega} l_i} \tag{12}$$

where ω is the number of the connected subgraphs, N_i represents the number of nodes and l_i indicates the average distance in the i^{th} connected subgraphs. The average distance of the connected subgraphs reflects the invulnerability; the smaller the average distance, the better the survivability. However, when there are too many connected subgraphs in the whole network, the network survivability will decrease sharply.

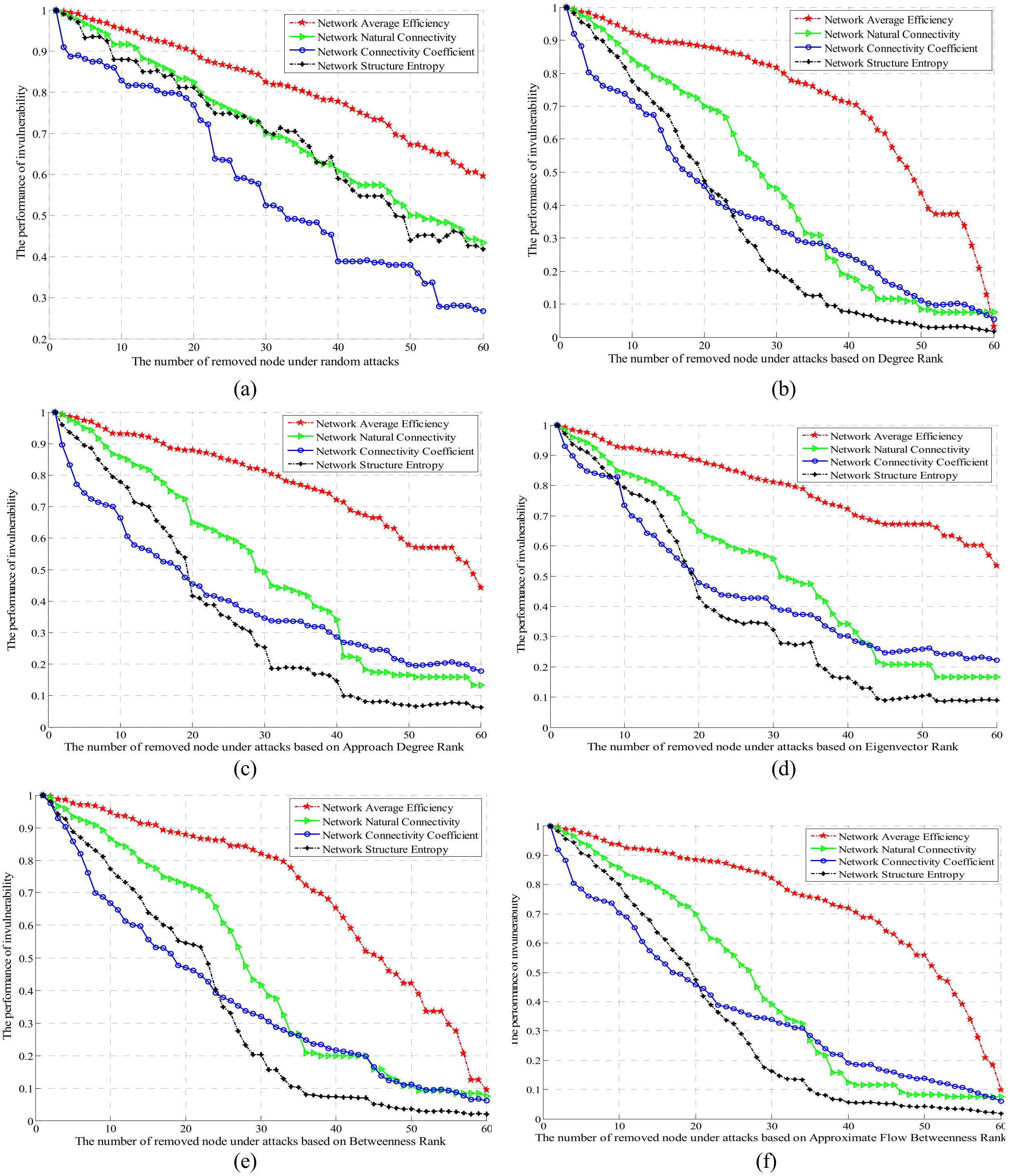
In the literature [18], [19], it has been proven that the natural connectivity and edge removal or addition are strictly monotonic, so the natural connectivity can be used to describe the network survivability. The natural connectivity of graph G is defined as:

$$\bar{\lambda} = In(\frac{1}{N}\sum_{i=1}^{N} e^{\lambda_i}) \tag{13}$$

where λ_i is the eigenvalue of adjacency matrix $A(G)$ which belongs to graph G.

The variation trend of invulnerability in a military heterogeneous network under six different attack strategies is shown as FIGURE 4. Furthermore, FIGURE 4 (a) shows the relationship between four invulnerability measures and random failure. FIGURE 4(a)-(f) shows the relationship between four invulnerability measures and different kind of deliberate attacks.

As shown in FIGURE 4, when the military heterogeneous network is under random attack, the variation trend of network structure entropy is relatively smooth, the curve is between the network average efficiency and network connectivity coefficient, which is close to network natural connectivity. This is due to the equal failure probability of each node in the military heterogeneous network, so the network



(a)

(b)

(c)

(d)

(e)

(f)

FIGURE 4. **Effect of network invulnerability by different attacks.**

invulnerability decays slowly. Network connectivity coefficient and improved Albert algorithm in [42] have a similar changing curve, and it modifies the error of Albert algorithm during the calculation of the network connectivity after a large attack [11], so the simulation work in this paper also supports the correctness of the research results in that literature [42].

When the military heterogeneous network is deliberately attacked, the increase in the number of attacked important nodes causes, the network invulnerability index to drop rapidly, raising the signigicance of deliberate attacks on network invulnerability. From the FIGURE 4, the decreasing trend of the network structure entropy is obviously faster than network average efficiency and network connectivity coefficient. In particular, after the first 20 important nodes are removed, the downtrend of network structure entropy is the same as network connectivity coefficient. However, when the number of removed nodes exceeds 20, the downward trend of network structure entropy is most obvious. This is because network invulnerability is less than 0.5 when the number of deliberately deleted nodes is more than 20, and the network communication capabilities are very poor. Thus, the results show that the network structure entropy is more sensitive than other invulnerability indices. In addition, when 20 nodes were deliberately attacked, the network structure entropy was already less than 0.5. When the number of deliberately removed nodes increased from 20 to 40, the network is at its most sensitive, with the largest drop is the network structure entropy. When the number of deliberately removed nodes is larger than 40, the network structure entropy is less than 0.2, there is almost no changes. This is because at this time many nodes become isolated nodes which cannot communicate properly, the network communication capabilities are very poor. In brief, the network structure entropy has high precision and can better reflect the invulnerability of a military heterogeneous network.

V. CONCLUSIONS

To characterize the needs of the information war, the form of the warfare changes from platform-centric to network-centric warfare, highlighting the confrontation between the two systems of systems (SoS) based networks. This paper proposes an invulnerability measure based on the network structure entropy for the military heterogeneous network, and establishes a network structure entropy model. Simulations analyze the impacts on the military heterogeneous network under random, deliberate and other kinds of attacks. Compared with other invulnerability measures, the measure proposed by this paper has high sensitivity and precision, and it is able to reflect the invulnerability of military heterogeneous networks. The research method of this paper provides a new research approach for the measurement and analysis of military heterogeneous network invulnerability. At the same time, the invulnerability measurement proposed in this paper can be used to evaluate the resilience capability of military networks.

So far, the present research has only focused on the static, single layer, non-interacting network model. In fact, the military heterogeneous network is a dynamic, interdependent network, liable to attack. To this end, the research on the invulnerability of the dynamic military heterogeneous network model or cascading failures on military heterogeneous network would be further research directions.

REFERENCES

[1] J.-W. Wang and L.-L. Rong, "Robustness of the western United States power grid under edge attack strategies due to cascading failures," *Saf. Sci.*, vol. 49, no. 6, pp. 807–812, Jul. 2011.

[2] Y.-S. Lan, Y. Kan, and W. Heng, "Delay assessment method for networked C4ISR system architecture," *Syst. Eng. Electron.*, vol. 35, no. 9, pp. 1908–1914, Sep. 2013.

[3] X. Song, W. Shi, G. Tan, and Y. Ma, "Multi-level tolerance opinion dynamics in military command and control networks," *Phys. A, Stat. Mech. Appl.*, vol. 437, pp. 322–332, Nov. 2015.

[4] H. Yu, Z. Liu, and Y. J. Li, "Using local improved structural holes method to identify key nodes in complex networks," in *Proc. 5th Conf. Meas. Technol. Mechatronics Autom.*, Hong Kong, Jan. 2013, pp. 1292–1295.

[5] N. Ghazisaidi, M. Scheutzow, and M. Maier, "Survivability analysis of next-generation passive optical networks and fiber-wireless access networks," *IEEE Trans. Rel.*, vol. 60, no. 2, pp. 479–492, Jun. 2011.

[6] G. Yan, T. Zhou, B. Hu, Z.-Q. Fu, and B.-H. Wang, "Efficient routing on complex networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 73, no. 4, pp. 046108-1–046108-4, Apr. 2006.

[7] S. Li, L. Li, Y. Yang, and Q. Luo, "Revealing the process of edge-based-attack cascading failures," *Nonlinear Dyn.*, vol. 69, no. 3, pp. 837–845, Aug. 2012.

[8] S. Li, L. Li, Y. Jia, X. Liu, and Y. Yang, "Identifying vulnerable nodes of complex networks in cascading failures induced by node-based attacks," *Math. Problems Eng.*, vol. 2013, pp. 938398-1–938398-10, Nov. 2013.

[9] D. Scheidt and K. Schultz, "On optimizing command and control structures," in *Proc. 16th Int. Command Control Res. Technol. Symp.*, Quebec City, QC, Canada, 2011, pp. 1–26.

[10] Z.-H. Qu, P. Wang, C.-M. Song, and Z.-G. Qin, "Enhancement of scale-free network attack tolerance," *China Phys. B*, vol. 19, no. 11, pp. 110504-1–110504-6, Jul. 2011.

[11] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, pp. 378–382, Jul. 2000.

[12] H. Wang, P. X. Liu, and P. Shi, "Observer-based fuzzy adaptive output-feedback control of stochastic nonlinear multiple time-delay systems," *IEEE Trans. Cybern.*, vol. 47, no. 9, pp. 2568–2578, Sep. 2017.

[13] X. Zhao, H. Yang, W. Xia, and X. Wang, "Adaptive fuzzy hierarchical sliding-mode control for a class of MIMO nonlinear time-delay systems with input saturation," *IEEE Trans. Fuzzy Syst.*, vol. 25, no. 5, pp. 1062–1077, Oct. 2016.

[14] H. Wang, W. Sun, and P. X. Liu, "Adaptive intelligent control of nonaffine nonlinear time-delay systems with dynamic uncertainties," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 47, no. 7, pp. 1474–1485, Jul. 2017.

[15] T. Zhang, X. Shi, Q. Zhu, and Y. Yang, "Adaptive neural tracking control of pure-feedback nonlinear systems with unknown gain signs and unmodeled dynamics," *Neurocomputing*, vol. 121, no. 18, pp. 290–297, Dec. 2013.

[16] K. Anand and G. Bianconi, "Entropy measures for networks: Toward an information theory of complex topologies," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 80, no. 2, pp. 045102-1–045102-4, Oct. 2009.

[17] L. Ming *et al.*, "A novel method for survivability test based on end nodes in large scale network," *KSII Trans. Internet Inf. Syst.*, vol. 9, no. 2, pp. 620–636, Feb. 2015.

[18] J. Wu, M. Barahona, Y.-J. Tan, and H.-Z. Deng, "Natural connectivity of complex networks," *Chin. Phys. Lett.*, vol. 27, no. 7, pp. 295–298, Jul. 2010.

[19] J. Wu, M. Barahona, Y.-J. Tan, and H.-Z. Deng, "Spectral measure of structural robustness in complex networks," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 41, no. 6, pp. 1244–1252, Nov. 2011.

[20] J. Wu, H.-Z. Deng, and Y.-J. Tan, "Spectral measure of robustness for Internet topology," in *Proc. 3rd IEEE Int. Conf. Comput. Sci. Inf. Technol.*, Chengdu, China, Jul. 2010, pp. 50–54.

[21] E. Estrada, N. Hatano, and M. Benzi, "The physics of communicability in complex networks," *Phys. Rep.*, vol. 514, no. 3, pp. 89–119, May 2012.

[22] Y.-L. Shang, "Local natural connectivity in complex networks," *Chin. Phys. Lett.*, vol. 28, no. 6, pp. 068903-1–068903-4, Jun. 2011.

[23] C. Wang, L. Li, and G. J. Chen, "An entropy theory based large-scale network survivability measurement model," in *Proc. IEEE Int. Conf. Netw. Infrastruct. Digit. Content*, Beijing, China, Sep. 2014, pp. 240–246.

[24] J. Rak, "Measures of region failure survivability for wireless mesh networks," *Wireless Netw.*, vol. 21, no. 2, pp. 673–684, Sep. 2015.

[25] X. Li, M. K. Ng, and Y. Ye, "MultiComm: Finding community structure in multi-dimensional networks," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 4, pp. 929–941, Apr. 2014.

[26] A. H. Dekker, "Analyzing C2 structures and self-synchronization with simple computational models," in *Proc. 16th Int. Command Control Res. Technol. Symp.*, Quebec City, QC, Canada, Jun. 2011, pp. 1–11.

[27] A. Tolk *et al.*, "Applying the Information age combat model: Quantitative analysis of network centric operations," *Int. C2 J.*, vol. 3, no. 1, pp. 1–25, Jan. 2009.

[28] S. Deller, G. Rabadi, A. Tolk, and S. R. Bowling, "Organizing for improved effectiveness in networked operations," in *Operations Research for Unmanned Systems*, vol. 17, J. R. Cares and J. Q. Dickmann, Eds. Hoboken, NJ, USA: Wiley, Mar. 2016, pp. 255–270.

[29] Q.-F. Bian, T.-T. Hang, H. Liu, and M.-Y. Fang, "Research on the diameter and average diameter of undirected double-loop networks," in *Proc. 9th Int. Conf. Grid Cloud Comput.*, Nanjing, China, Nov. 2010, pp. 461–466.

[30] C.-C. Yen, M.-Y. Yeh, and M.-S. Chen, "An efficient approach to updating closeness centrality and average path length in dynamic networks," in *Proc. IEEE 13th Int. Conf. Data Mining*, Dallas, TX, USA, Dec. 2013, pp. 867–876.

[31] C. Wang, D. Wang, and Y. Dai, "Towards a unified framework for network survivability measurement," in *Proc. 2nd Int. Conf. Netw. Secur., Wireless Commun. Trusted Comput.*, Hubei, China, Apr. 2010, pp. 129–134.

[32] S.-C. Peng, W.-J. Jia, and G.-J. Wang, "Survivability evaluation in large-scale mobile Ad-Hoc networks," *J. Comput. Sci. Technol.*, vol. 24, no. 4, pp. 761–774, Jul. 2009.

[33] L. Ming, D. Wang, L. Zhang, X. Kuang, J. Tang, and C. Wang, "Index system of network security and survivability," in *Proc. Int. Conf. Instrum., Meas., Comput., Commun. Control*, Beijing, China, Oct. 2011, pp. 848–851.

[34] X.-J. Yu and S. Wang, "Measuring the network efficiency and the component importance for multiclass transportation network," in *Proc. 2nd Int. Conf. Inf. Sci. Control Eng.*, Shanghai, China, Apr. 2015, pp. 801–804.

[35] A. H. Dekker, "Measuring the agility of networked military forces," *J. Battlefield Technol.*, vol. 9, no. 1, pp. 19–24, Mar. 2006.

[36] S. Yang and Z. Zhang, "Entropy weight method for evaluation of invulnerability in instant messaging network," in *Proc. Internet Comput. Sci. Eng.*, Harbin, China, Dec. 2010, pp. 239–243.

[37] H.-G. Hwang, H.-K. Kim, and J.-S. Lee, "An agent based modeling and simulation for survivability analysis of combat system," *J. Korea Inst. Inf. Commun. Eng.*, vol. 16, no. 12, pp. 2581–2588, Dec. 2012.

[38] K. Al-Begain, A. Dudin, V. Klimenok, and S. Dudin, "Generalized survivability analysis of systems with propagated failures," *Comput. Math. Appl.*, vol. 64, no. 12, pp. 3777–3791, Dec. 2012.

[39] S. Parvin, F. K. Hussain, J. S. Park, and D. S. Kim, "A survivability model in wireless sensor networks," *Comput. Math. Appl.*, vol. 64, no. 12, pp. 3666–3682, Dec. 2012.

[40] X. He and Y. Wu, "Analysis of supply chain system stability based on network structure entropy," in *Proc. Int. Conf. Mech. Sci., Electr. Eng. Comput.*, Jilin, China, Aug. 2011, pp. 1326–1330.

[41] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.

[42] S. He, J. Cao, W. He, and Q. Liu, "A measure method for network invulnerability based on improved Albert Algorithm," in *Proc. Int. Conf. Instrum., Meas., Comput., Commun. Control*, Beijing, China, Oct. 2011, pp. 812–815.

XIUE GAO was born in Dalian, Liaoning, in 1976. She received the B.Sc. and M.Sc. degrees from the Dalian University of Technology in 2002 and 2005, respectively.

She is currently pursuing the Ph.D. degree with the School of Computer Science and Technology, Dalian University of Technology, Dalian, China. Her research interests are mainly within the field of internet technology and intelligent control.

KEQIU LI (SM'04) was born in Dalian, Liaoning, in 1971. He received the Ph.D. degree from the Graduate School of Information Science, Japan Advanced Institute of Science and Technology, in 2005, and the B.Sc. and M.Sc. degrees from the Department of Applied Mathematics, Dalian University of Technology, in 1994 and 1997, respectively.

He also has two-year postdoctoral experience with the University of Tokyo, Japan, from 2005 to 2007. He has been a Professor of computer science with the School of Computer Science and Technology, Dalian University of Technology, China, since 2007. He is a Ph.D. Tutor of computer science with the Dalian University of Technology, Dalian, Liaoning. He has authored over 100 technical papers in computer network and security, web technology, multimedia application, mobile agent technology and grid computing, many of them are in top tier high impact journals, such as the IEEE TPDS, the ACM TOIT, and the ACM TOMCCAP. His main research interests are internet technology, data center networks, cloud computing and wireless networks.

Prof. Li was a recipient of the National Outstanding Youth Funds in 2012. He has chaired international conferences, and he is also a reviewer for several reputable international journals and a committee member of several international conferences. He is an Associate Editor of the IEEE TPDS and the IEEE TC.

BO CHEN was born in Wusheng, Sichuan, in 1972. He received the B.Sc. degree from the Hubei University of Automotive and Technology, Shiyan, China, in 1999, and the M.Sc. and Ph.D. degrees from the Dalian University of Technology, Dalian, China, in 2002 and 2005, respectively.

He has been a Professor of control science and engineering with the School of Information and Engineering, Dalian University, Dalian, China, since 2007. He is a Distinguished Professor in Liaoning province. He is a Ph.D. Tutor of control science and engineering with the Changchun University of Science and Technology, Changchun. He has authored over 50 journal and conference papers in complex network, command and control network, human body composition, fault diagnosis, machine learning, and data mining, many of them are in top tier high impact journals. His main research interests are computer network, command and control network, complex network.

Prof. Chen received the National Science and Technology Progress Award in 2011. He is a reviewer for several reputable international journals and committee member of several international conferences.