Journal of Information Hiding and Multimedia Signal Processing ©2016 ISSN 2073-4212
Ubiquitous International Volume **7**, Number **6**, November **2016**

Information Entropy and Cross Information Entropy Based Attacking Methods for Complex Networks

Zhe-Ming Lu* and Ya-Pei Feng

School of Aeronautics and Astronautics
Zhejiang University
Hangzhou, 310027, P. R. China
*Coresponding Author: zheminglu@zju.edu.cn

Received March, 2016; revised July, 2016

Abstract. *The security issue of complex networks has drawn significant concerns recently and there exist many papers doing research works on how to improve the attacking efficiency. Behaviors of complex networks under intentional attacks guided by degree or betweenness centrality have been extensively studied, however, these attack strategies do not act well for the small-world network or the scale-free network. In this paper, we do research works on how different attacking methods affect the characteristics of complex networks. In our simulation tests, we remove nodes in three different ways: ranking the information entropy of each node from high to low and deleting nodes according to the order, or ranking the cross information entropy of each node from high to low and deleting nodes according to the order, or deleting nodes randomly. With regard to the complex networks without node capacity, our evaluation criterion is based on the network attack efficiency, that is, the relative size of the giant connected subgraph of the network. Our understanding about damage attack may also shed light on efficient solutions to protect real networks against damage attack.*
Keywords: Complex networks, Information entropy, Cross information entropy, Giant connected component.

1. **Introduction.** In real life, many economic networks, social networks, electrical power grids, transportation networks and the Internet are all complex networks, which are also widely studied in many subjects. Complex networks are used to describe the physical, biological and social phenomena and we can establish the forecast model of these phenomena or analysis model. Then we can use the static and/or dynamic characteristics of the network to explain these phenomena[1].

Network survivability refers to the ability of keeping normal communication in the event of failures, it is not related to the reliability of the network nodes and edges. The research shows that different network models show great difference in invulnerability under different attacks. The measure of network invulnerability is a kind of quantitative indicator, so choosing an appropriate measure is the basis of improving the attacking efficiency of complex networks.

Static geometric features of complex networks are usually measured by its internal relationship among nodes, such as the average distance, degree distribution, the clustering coefficient, the diameter and so on. Recently, Cao et al. [2] studied the entropy of degree distribution in scale-free networks and found that the entropy of the degree distribution is an effective measure of the network resilience to random failures, they also found that the sum of the entropy of the degree distribution could better reflect the characteristics of the

heterogeneity of complex networks. Besides, according to the definition of information entropy and its physical significance, the information entropy of nodes can reflect the status of nodes in disseminating information in complex networks. In 2012, Srivastava et al. [3] discussed the difference between network structure parameters and the performance of network survivability. With regard to attacking strategies, Wang et al.[4] attacked the Internet or other actual networks by attacking the nodes and edges. In the literature, Wu et al. [5] analyzes the invulnerability of complex networks whose local topology information is known, and compared the effectiveness of a variety of selective attacking methods, however its attack efficiency is not the best.

To solve this problem, this paper proposes the information entropy and cross information entropy derived from the degree of nodes to guide the network attack process, and we adopt the relative size of the giant connected subgraph to evaluate the attacking efficiency.

2. Problem Statement and Preliminaries.

2.1. Survivability Measure of Complex Networks.

To measure the survivability of complex networks we can use various measurement indices, such as degree, clustering coefficient, betweenness, connectivity, average shortest path, and the largest connected subgraph. In our experiment, we choose the connected subgraph as the survivability measure of a complex network. A connected subgraph is a subgraph of the network, and there must be at least one path between two nodes. For an unconnected graph, it can be divided into at least two connected subgraph. And we define the connected subgraph with the maximum number of nodes as the giant connected component or giant connected subgraph. With the removal of nodes in the complex network, the topology of the complex network will be changed, and the network will be divided into many subgraphs. So we focus on the change in the size of the giant connected subgraph to evaluate the fragment of the complex network. The relative size of giant connected subgraph is defined as follows:

$$W = \frac{S}{N} \tag{1}$$

Here S is the number of nodes in the giant connected subgraph, and N is the total number of nodes in the complex network. The smaller the W, indicating the network survivability is weak, the higher the attack efficiency of the attacking method.

2.2. Definition of Information Entropy.

The concept of entropy originates in physics, which is used to measure the disorder degree of a thermodynamical system. If the system tends to be disorderly, its entropy increases towards 1; if the system tends to be orderly, its entropy decreases towards 0. From the point view of information theory, entropy is the measurement of uncertainty. The higher the entropy is, the more amount of information it carries, and the lower the entropy is, the less amount of information it can be transmitted. In information theory, entropy can be defined as follows: Shannon defined the entropy H of a discrete random variable $\mathbf{X}$ with possible values $x_1, ..., x_n$:

$$H(\mathbf{X}) = E(I(\mathbf{X})) \tag{2}$$

Here E is the expectation operator, and $I(\mathbf{X})$ is the information content of $\mathbf{X}$. $I(\mathbf{X})$ is itself a random variable. When taken from a finite sample, the entropy can explicitly be written as[6]:

$$H(\mathbf{X}) = \sum_{i=1}^{n} p(x_i) * I(x_i) = -\sum_{i=1}^{n} p(x_i) * \log_b p(x_i) \tag{3}$$

Where p is the probability mass function of $\mathbf{X}$, and the typical value of b is 2, Euler's number e, or 10, and the unit of entropy is bit for $b = 2$, nat for $b = e$, and hartley for $b = 10$. Here, we set it as $b = 10$.

In complex networks, the amount of information can be defined as the number of adjacent nodes connected to the node, which is the degree k_i of a node. So the probability mass function can be expressed as $I_i = \frac{k_i}{\sum_{i=1}^{N} k_i}$, and $\sum_{i=1}^{N} k_i$ is the sum of degree of the network. Then for a complex network, the information entropy of a node can be defined as follows:

$$Ent_i = -\frac{k_i}{\sum_{i=1}^{N} k_i} * \lg(\frac{k_i}{\sum_{i=1}^{N} k_i}) \tag{4}$$

According to the definition of information entropy, a node with larger information entropy has more stronger relationship with other nodes. So if we attack nodes according to the order of information entropy of nodes, we can expect to attack the network more faster than random attacking.

2.3. **Definition of Cross Information Entropy.** In probability theory, a conditional probability measures the probability of an event given that another event has occurred. For discrete event system, cross information entropy can be defined as: there are two events p_1 and p_2, and if event p_1 happened under the condition of the event p_2, the cross entropy is $E(p_1|p_2) = p_1 \ln(\frac{p_1}{p_2})$; if event p_2 happened under the condition of the event p_1, the cross entropy is $E(p_2|p_1) = p_2 \ln(\frac{p_2}{p_1})$; then we can get $E(p_1, p_2) = E(p_1|p_2) + E(p_2|p_1)$. Here in discrete event system p denotes the event occurrence probability.[7]

Compared to the information entropy of a single event, the cross information entropy can better reflect the relationship among nodes, which has obvious advantage in measuring the importance of nodes. So for a complex network, the cross information entropy of a node can be defined as $crosEnt_i$ as follows[8]:

$$crosEnt_i = -\sum_{j \in M} \frac{k_i}{\sum_{i=1}^{N} k_i} * \lg(\frac{k_i}{k_j}) \tag{5}$$

Here, M is the set of adjacent nodes of Node i. As the same to the definition of information entropy, k_i is the degree of the Node i, and $\sum_{i=1}^{N} k_i$ is the sum of degree of the network.

3. **Description of Network Attacking.** As early as 2000, Albert et al. [9] did research works on the invulnerability of complex networks and they focused on how the network topological structure affects the survivability of complex networks. In their simulation, they deleted nodes in random (ER) networks and scale-free (BA) networks in two different methods. In the first method, they removed nodes randomly from the network; In the second method, they removed nodes according to the connection degree of nodes from large to small. Then they tested the change in diameter of a network to assess the degree of network fragmentation. Thus they found that the scale-free networks under random attacking have a stronger anti-damage ability; but under deliberate attacking, the scale-free networks would be attacked to collapse more easily than random networks. In 2008, Bao et al [10] did research works on scale-free (BA) networks and investigated the dynamics of load entropy during failure propagation using a new cascading failure load model, and their research works showed that the load entropy for a large cascading failure increases much more sharply than that for a small one and then the large cascading failures can be identified at the early stage of failure propagation according to load entropy. Thus,

we believe that the load entropy can be used as an index to be optimized in cascading failure control and defense in many real-life complex networks.

Complex networks are usually faced with two kinds of attacks: random attacks and intentional attacks. Intentional attacks are also named as selective attacks. In a complex network, when a node is attacked, then the node and the edges connected to it are all deleted. There exist many kinds of attacking methods[9]: initial degree based attacking, initial betweenness based attacking, recalculated degree based attacking and recalculated betweenness based attacking and so on. Here, we use three kinds of attacking methods: random attack, max information entropy based attacking and max cross information entropy based attacking.

(1) Random attack(RA for short): we attack nodes in the network randomly every time, and the final result is the average of the ten calculations. (2)Max information entropy based attacking(MIEA for short): we rank the information entropy of each node from high to low and delete nodes according to the order. (3) Max cross information entropy based attacking(MCIEA for short): we rank the cross information entropy of each node from high to low and delete nodes according to the order.

Firstly we calculate the initial connected subgraph and get the initial giant connected subgraph of the network. Then we attack nodes in a specific turn: each time we remove a node, and then recalculate the current giant connected subgraph of the new network formed by the remaining nodes. Finally, we keep attacking until the network is attacked to completely collapse. After each attack, according to Eq. (1) we calculate the relative size of the giant connected subgraph to compare the attack efficiency of the three attack methods. We set N_r as the number of nodes which has already been removed, and N as the initial size of the complex network. So we denote the ratio of nodes which are removed from the network as K:

$$K = \frac{N_r}{N} \tag{6}$$

4. **Simulation Results and Analysis.** In our simulation tests, we choose the Zachary karate club network (Zachary network), small-world (ws network) networks and scale-free (BA network) networks to evaluate the effectiveness of the proposed schemes.

4.1. **Simulation Results on the Zachary Karate Club Network.** In our simulation, firstly we take the Zachary karate club network (Zachary network) as an example in Fig. 1. The Zachary network is a social network of friendships between 34 members of a karate club at a US university in the 1970s which is widely used as a research example. There are 34 nodes and 78 edges in this network, and each node in the network, respectively, indicates a member of the club. The edges between nodes indicate that the nodes often occur together in club activities, such as karate training, club meetings, etc. In the course of the investigation, the club is divided into 2 small clubs, each of which is the core of the club, which is divided into small clubs, such as the A. John (Node 34) and coach Hi Mr. (Node 1). The results under three different attacking methods are shown in Fig. 2.

From the changes in the relative size of giant connected subgraph under different attacking methods in Fig. 2, we can see that the relative size of giant connected subgraph decreases more faster under the attacking method based on information entropy and the attacking method based on cross information entropy. So we can know the attack efficiency of our proposed methods are much higher.

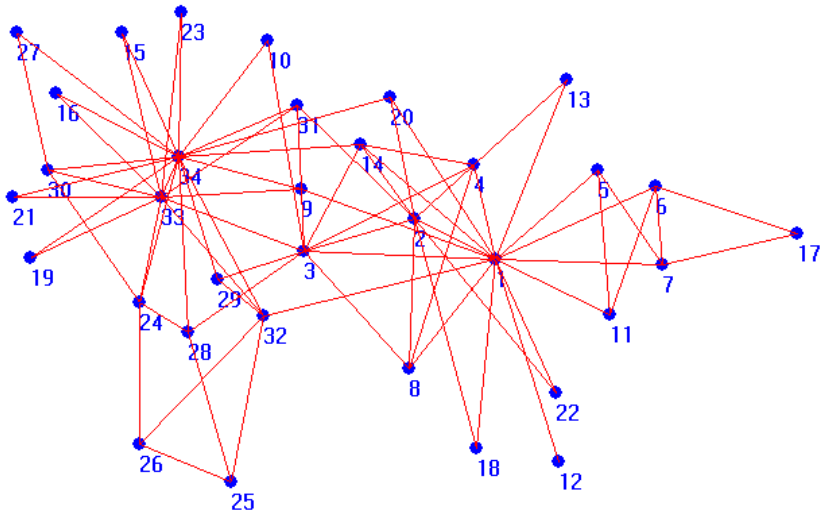

FIGURE 1. Zacharya karate club network

4.2. **Simulation Results on Small-world Networks.** Next, we take small-world networks (WS network) as our test examples. A small-world network is a type of mathematical graph in which most nodes are not neighbors of one another, but most nodes can be reached from every other by a small number of hops or steps. Specifically, a small-world network is defined to be a network where the typical distance L between two randomly chosen nodes (the number of steps required) grows proportionally to the logarithm of the number of nodes N in the network. Small-world properties are found in many real-world phenomena, including websites with navigation menus, food chains, electric power grids, metabolite processing networks, networks of brain neurons, voter networks, telephone call graphs, and social influence networks.

Here, we choose the WS networks with different numbers of nodes (100 and 1000) to do simulations. For the WS network with 100 nodes, the number of original nodes is 100, the connection probability is 0.1, and the number of neighbors is 4. For the WS network with 1000 nodes, the number of original node is 1000, connection probability is 0.1, and the number of neighbors is 4. The results are shown in Fig. 3 and Fig. 4 respectively.

To further demonstrate the superiority of our schemes, we also do simulations on the small-world networks (WS netwrok) with different numbers of nodes: 200, 400, 600, 800, 1000. The comparison results are shown in Fig. 5, where W is the relative size of giant connected subgraph and N is the total number of nodes in the WS network. When the relative size of giant connected subgraph decreases to 0.25, the network is about to collapse. So we record the ratio of the number of nodes removed when the relative size of giant connected subgraph decreases to 0.25. Because the effects of the two methods based on MIEA and MCIEA are almost the same, we only show the attacking efficiency of the attacking method based on MIEA and random attack.

From above results, we can see that when a node is removed from the network, the edges connected to it will also be removed. Thus it leads to the network broken into many

connected subgraphs and the size of the giant connected subgraph will decrease. Two conclusions can be drawn as follows:(1)As to a WS network, when the size of connected subgraph decreases to the same degree, our attacking method based on max information entropy or the method based on the max cross information entropy need fewer number of attacks.(2)The greater the network is, the higher the efficiency of our methods is. So our method are very suitable for attacking real networks.

From above results we can see that, for WS networks, the attack efficiency of the three attack methods is ranked as MCIEA>MIEA>RA. In our methods, when the ratio of nodes which are removed decreases into the range between 0.4 and 0.5, the network nearly collapses. While in the random attack method, the ratio of nodes which are required to be removed is much higher.

4.3. **Simulation Results on Scale-free Networks.** Finally, we test the attack efficiency of our methods based on scale-free networks. A scale-free network is a network whose degree distribution follows a power law, at least asymptotically. The most notable characteristic in a scale-free network is the relative commonness of nodes with a degree that greatly exceeds the average. The highest-degree nodes are often called "hubs", and are thought to serve specific purposes in their networks, although this depends greatly on the domain. The scale-free property strongly correlates with the network's robustness to failure. It turns out that the major hubs are closely followed by smaller ones.

Here, we choose the scale-free networks (BA network) with different numbers of nodes (100 and 1000) to do simulations. For the BA network with 100 nodes, the number of original node is 20, the number of iterations is 80, and the network connects to 4 old nodes at each iteration. For the BA network with 1000 nodes, the number of original node is 20, the number of iterations is 980, and the network connects to 4 old nodes at each iteration. The results are shown in Fig. 6 and Fig. 7 respectively.

To further demonstrate the superiority of our schemes, we also do simulations on the BA networks with different numbers of nodes: 200, 400, 600, 800, 1000. The comparison results are shown in Fig. 8, where W is the relative size of giant connected subgraph and N is the total number of nodes in the BA network. When the relative size of giant connected subgraph decreases to 0.25, the network is about to collapse. So we record the ratio of the number of nodes removed when the relative size of giant connected subgraph decreases to 0.25, and then we can analyze the attacking efficiency of two different attacking methods. Because the effects of the two methods based on MIEA and MCIEA are almost the same, we only show the attacking efficiency of the attacking method based on MIEA and random attack.

From above results we can see that, for the BA network, the attack efficiency of the three attack methods is ranked as MCIEA>MIEA>RA. Compared to the WS networks, when the BA network nearly collapses, the ratio of nodes which are required to be removed is lower. Because the degree distribution of the BA network follows the power law, which determines the robustness of the network, while the degree distribution of the WS network is a narrow distribution.

5. **Conclusions.** In this paper, we propose two network attacking methods based on information entropy and cross information entropy to improve network attacking efficiency. Simulation results show that the attacking efficiencies based on information entropy and cross information entropy for a large cascading failure are much higher than random attacking, especially in small-world networks. This is because the degree distribution of small world networks is a narrow distribution, and there are many nodes having the same node degree. The survivability under attacking of small-world networks and scale free

networks are different because of different network topologies. These differences have important reference value to attack real networks. Besides, the experiment results indicate that the cascading failures in WS networks and BA networks, triggered by initial attacks on a single node, but spreading to the entire network, is one of the intriguing problems. Different from most of previous methods, our new efficient methods based on information entropy and cross information entropy can represent the node removal mechanism in many real-life networks, which are significant in complex network attack or complex network defense.

To sum up, we believe that information entropy and cross information entropy can be used as indices in cascading failures control and defense in many real-life complex networks and we will do more research on them in the future.

REFERENCES

[1] J.Yan, H. He, Y.Sun, Integrated security analysis on cascading failure in complex networks, *IEEE Transactions on Information Forensics and Security*, vol.9, no.3, pp. 451–463, 2014.

[2] S.Cao, M.Dehmer, Y.Shi, Extremality of degree-based graph entropies, *Information Sciences*, vol.278, pp.22–33, 2014.

[3] A.Srivastava, B.Mitra, N.Ganguly, F.Peruani, Correlations in complex networks under attack, *Physical Review E*, vol.86, no.3, 2012.

[4] J.Wang, L.Rong, L.Zhang, Z.Z.Zhang, Attack vulnerability of scale-free networks due to cascading failures, *Physica A: Statistical Mechanics and its Applications*, vol.387, no.26, pp.6671–6678, 2008.

[5] J.Wu, H.Z.Deng, Y.J.Tan, D.Z.Zhu, Vulnerability of complex networks under intentional attack with incomplete information, *Journal of Physics A: Mathematical and Theoretical*, vol.40, no.11, pp.2665, 2007.

[6] M. Borda, Fundamentals in Information Theory and Coding[M]. Springer Berlin Heidelberg, 2011.

[7] B.Tellenbach, M.Burkhart, D.Schatzmann, D.Gugelmann, D.Sornette, Accurate network anomaly classification with generalized entropy metrics, *Computer Networks*, vol.55, no.15, pp.3485–3502, 2011.

[8] P-T.de.Boer, D.P.Kroese, S.Mannor, Y.Reuven, A tutorial on the cross-entropy method *Annals of operations research*, vol.134, no.1, pp.16–67,2005.

[9] P.Crucitti , V.Latora, M.Marchiori , Error and attack tolerance of complex networks, *Physica A: Statistical Mechanics and its Applications*, vol.340, no.1, pp.388–394, 2004.

[10] Z.J.Bao, Y.J.Cao, L.J.Ding, Dynamics of load entropy during cascading failure propagation in scale-free networks, *Physics Letters A*, vol.372,no.36, pp.5778–5782, 2008.

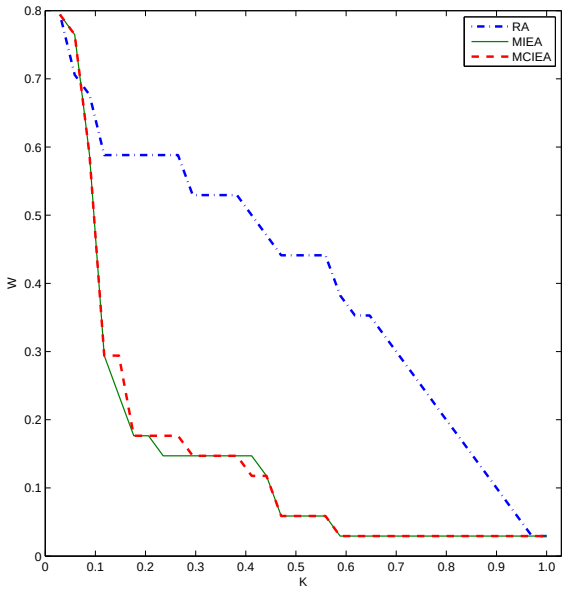

FIGURE 2. The change in the relative size of giant connected subgraph under different attacking methods for the Zachary network.

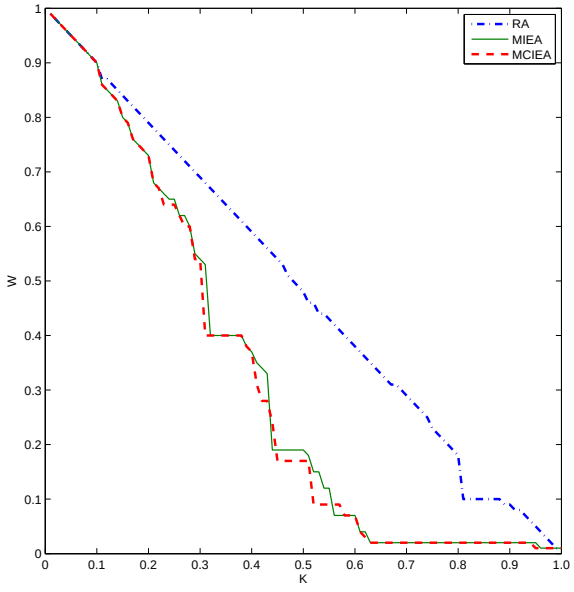

FIGURE 3. The change in the relative size of giant connected subgraph under different attacking methods for the WS network with 100 nodes.

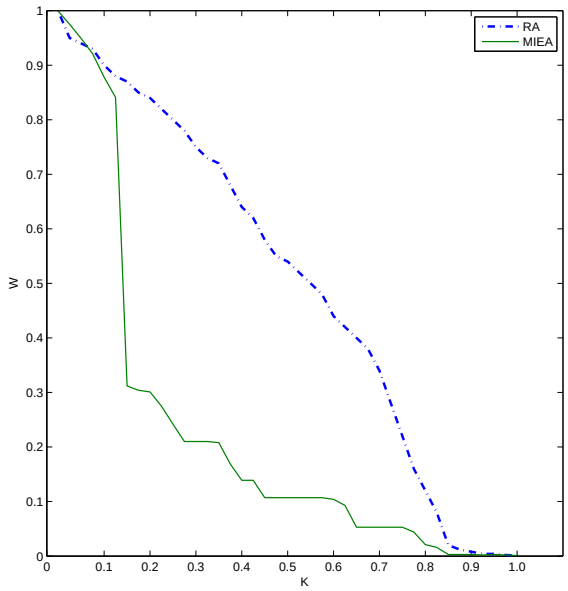

FIGURE 4. The change in the relative size of giant connected subgraph under different attacking methods for the WS network with 1000 nodes.

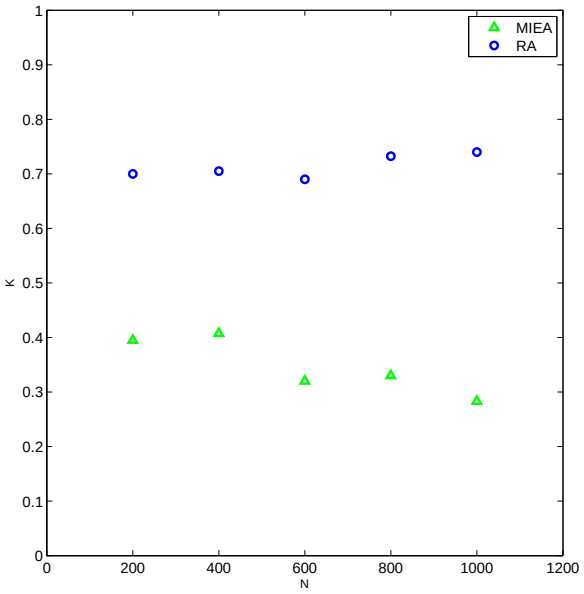

FIGURE 5. The comparison of attacking efficiency between the random attack method and our method for WS networks with different sizes when W decreases to 0.25

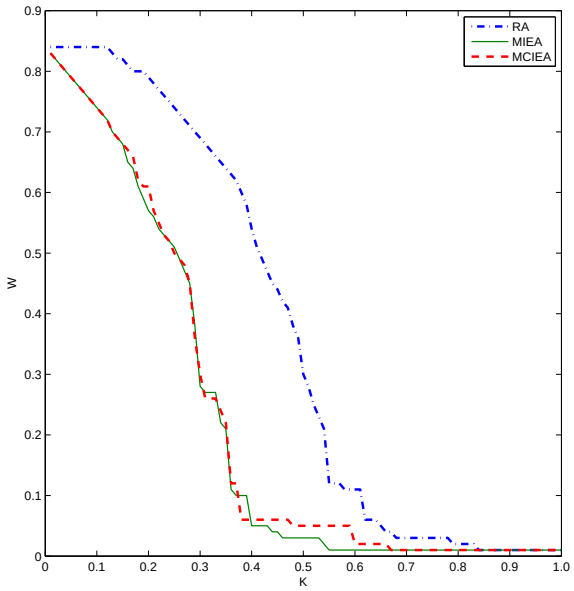

FIGURE 6. The change in the relative size of giant connected subgraph under different attacking methods for the BA network with 100 nodes.

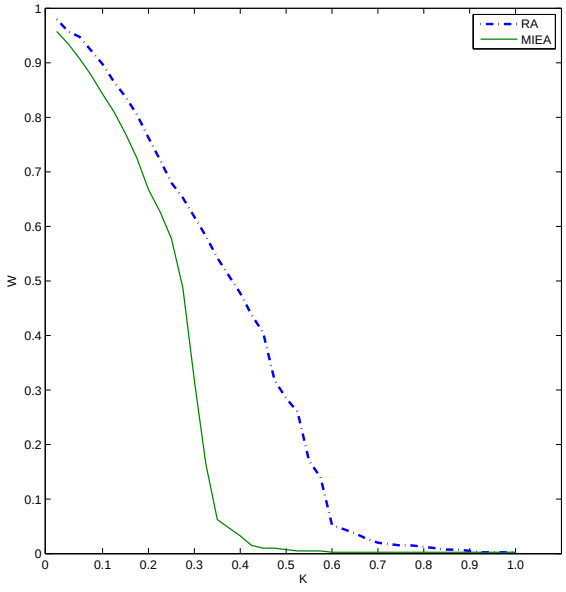

FIGURE 7. The change in the relative size of giant connected subgraph under different attacking methods for the BA network with 1000 nodes.

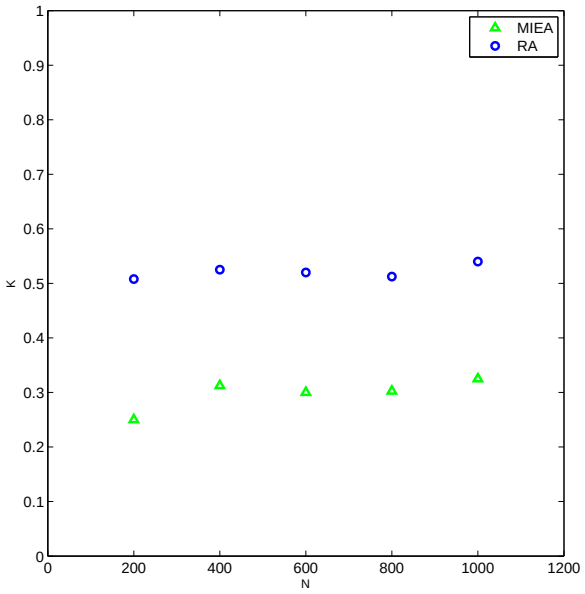

FIGURE 8. The comparison of attacking efficiency between the random attack method and our method for BA networks with different sizes when W decreases to 0.25