IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 23, 2020, accepted September 8, 2020, date of publication September 18, 2020,
date of current version September 30, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3024942

Robustness of Complex Networks Considering Attack Cost

CHENGWANG WANG AND YONGXIANG XIA, (Senior Member, IEEE)
School of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China

Corresponding author: Yongxiang Xia (xiayx@hdu.edu.cn)

This work was supported in part by the Laboratory of Science and Technology on Integrated Logistics Support, China.

ABSTRACT Robustness of complex networks has attracted much attention in diverse disciplines. Most of previous studies did not consider the attack cost. In this paper, the network robustness is studied with the consideration of attack cost, with different complex network models and different robustness indices. It is found that with different cost function and attack budget, the best attack strategy changes. When the budget is low and attacking hubs costs much more than attacking an unimportant node, then the high-degree attack (HDA) strategy performs worse than the low-degree attack (LDA) strategy. On the contrary, HDA is always a better strategy when the budget is high. Therefore, there is an intersection before and after that different attack strategies perform better. The position of this intersection is affected by the network structure, robustness index, cost function and the budget.

INDEX TERMS Attack cost, complex networks, robustness.

I. INTRODUCTION

Large-scale infrastructure networks, such as the Internet, transportation networks, power grids play important roles in our society [1]–[3]. In order to improve their performance and avoid unexpected damages, either due to random failures or intentional attacks, it is essential to study the robustness of such infrastructure networks. However, these networks usually have large scales and complex structures, which make the modeling and analysis difficult.

Recent progress in network science provides an efficient way for the study on the robustness of complex infrastructure networks [4]–[6]. Network science focuses on the structural properties of networks. Although different networks have different properties, they all can be demonstrated by structural elements such as nodes and links. More interestingly, many distinct networks have quite similar structural properties. And it has been shown that these properties are vital to determine the dynamics performed in the network.

The study on the robustness of complex networks has attracted much attention in the past two decades [7]–[12]. One common method is that the attacker is supposed to remove a proportion of nodes, and the robustness is measured by the connectivity of the rest network. It has been shown that scale-free networks are robust against random attack but fragile to intentional attack [13]. In such studies, the intentional attack is conducted on hubs, which are supposed to be the most important nodes in the network, such as those with the highest degrees. Obviously, the removal of these nodes makes the network disconnected easily. In comparison, the homogeneous random graph is robust to both random failure and intentional attack.

In the above studies, it is assumed that the attacker pays the same cost to remove one node, no matter it is the hub or a remote unimportant node. In the real case, however, the removal of different node usually costs differently, and the intentional removal of a hub usually costs much more than the removal of an unimportant node. Based on this fact, some researchers studied different attack strategies with the consideration of attack cost. Zheng *et al.* [14] found that, when the attack cost is taken into account, the scale-free networks may be robust against intentional attacks. This finding is quite different from the famous "robust-yet-fragile" property of scale-free networks, as the latter did not consider the attack cost. Hong *et al.* [15] considered different attack strategies including the high-degree removal strategy (HDRS), low-degree removal strategy (LDRS), and the random removal strategy (RRS), and studied how the total attack cost and network assortativity coefficient affect the performance of different attack strategies. Zhang *et al.* [16]

The associate editor coordinating the review of this manuscript and approving it for publication was Yang Tang.

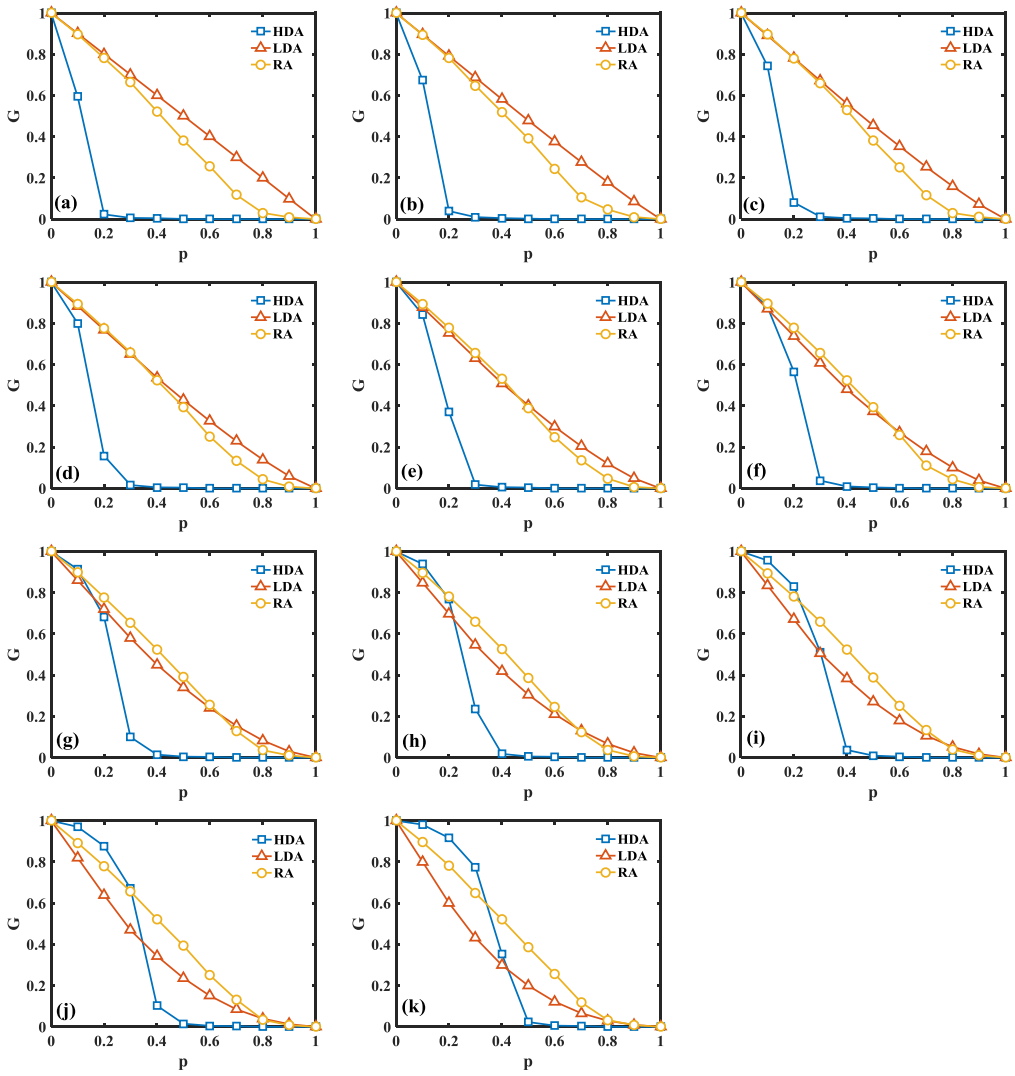

FIGURE 1. The relative size of the largest connected component G when considering the attack cost. (a) a=0; (b) a=0.1; (c) a=0.2; (d) a=0.3; (e) a=0.4; (f) a=0.5; (g) a=0.6; (h) a=0.7; (i) a=0.8; (j) a=0.9; (k) a=1. BA scale-free network with N=1000 and $\langle k\rangle \approx 4$ is considered. Each point is the average of 10 runs.

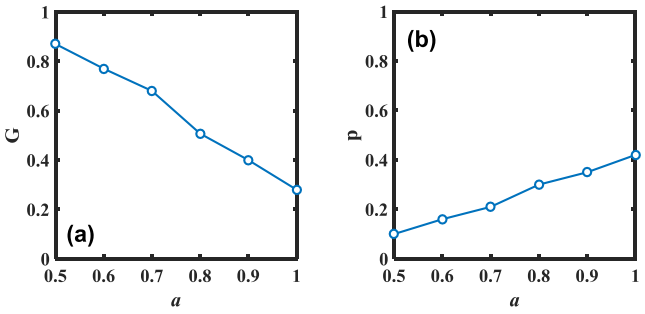

FIGURE 2. The intersection between HDA and LDA curves in figure 1. (a) the relative size of the largest connected component G at the intersection, as a function of a. (b) the budget p at the intersection, as a function of a. BA scale-free network with N=1000 and $\langle k\rangle \approx 4$ is considered. Each point is the average of 10 runs.

designed an optimization algorithm to defend the network from attacks when the cost is considered.

When considering the attack cost, there are actually two issues. One is the cost to remove an individual node. Obviously, the removal of a hub node should cost more than the removal of an unimportant node. Another issue is the total cost the attacker can pay. In this paper, we will consider both these two issues and study how these two issues affect the robustness of networks.

The rest of paper is organized as follows. In section II, the complex network models, the cost formulation and the robustness index are given. In section III, simulated results and discussions are provided. Finally, the work is concluded in section IV.

II. MODEL

A. NETWORK MODELS

Two network models are considered in this paper. One is the Barabasi-Albert (BA) scale-free network [17]–[19], and the

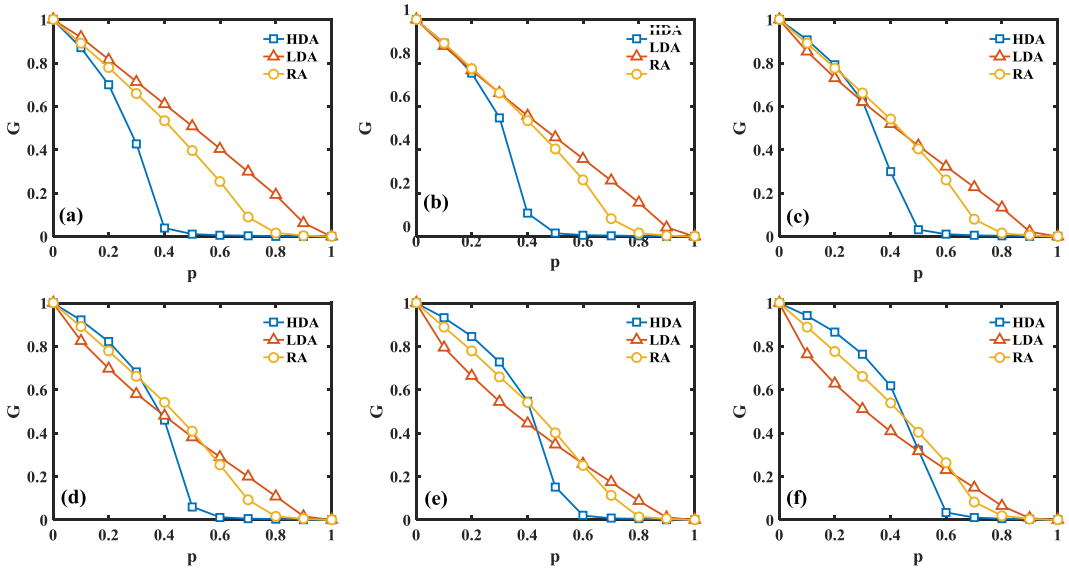

FIGURE 3. The relative size of the largest connected component G when considering the attack cost. (a) a=0; (b) a=0.2; (c) a=0.4; (d) a=0.6; (e) a=0.8; (f) a=1. ER random graph with N=1000 and $<k>$=4 is considered. Each point is the average of 10 runs.

other is the Erdos-Renyi (ER) random graph [20], [21]. These two network models show quite different characteristics in structure. The BA scale-free network model has the characteristics of growth and preferential attachment. As a result, the hub nodes have a large number of connections whereas most of other nodes only have few links. In this way, different nodes take quite different roles in the network. So, the BA scale-free network model generates heterogeneous network. In comparison, the nodes of the ER random graph model are connected with the same probability. Therefore, the ER random graph generates homogeneous network, where all nodes show identical property statistically. These two models are described in detail as follows.

1) BA SCALE-FREE NETWORK

Initially there are $m0$ nodes in the network. They are fully connected from one to another. Then at each time step, one node is added into the network, and this new node is connected to m existing nodes. The connection is based on a preferential rule. More specifically, the probability that a new node is connected to an existing node i is

$$\prod_i = \frac{k_i}{\sum_i k_i} \tag{1}$$

where k_i is the degree of node i. Repeat this growth process until the number of nodes reaches N. Denote the average degree of node as $<k>$.

2) ER RANDOM GRAPH

Initially there are N isolated nodes without any connection between each other. Then the links are randomly added between nodes, until the average degree reaches $<k>$.

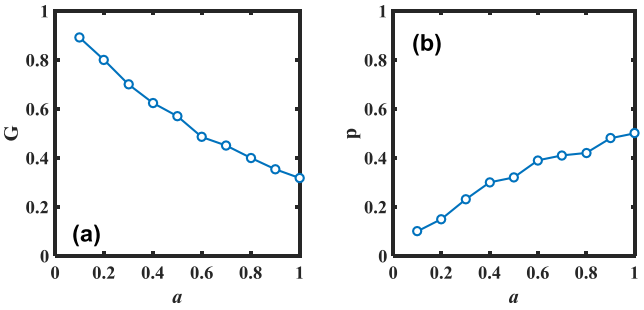

FIGURE 4. The intersection between HDA and LDA curves in figure 3. (a) the relative size of the largest connected component G at the intersection, as a function of a. (b) the budget p at the intersection, as a function of a. ER random graph with N=1000 and $<k>$=4 is considered. Each point is the average of 10 runs.

B. ATTACK COST

When the attacker removes a node from the network, a cost has to be paid. Generally speaking, the more important the node is the higher cost the attacker has to pay. In order to investigate the impact of attack cost on the robustness of network, define the cost to remove node i as

$$Y_i = k_i^a \tag{2}$$

where a is the cost factor. When $a = 0$, then the cost to remove different nodes is the same. This is equivalent to the traditional study where no cost is considered. Usually a should be positive, indicating the fact that removing a more important node costs more.

After defining the cost to remove a node, the attacker can conduct the attack and remove nodes. Here we consider three node attack strategies, i.e., HDA, LDA and RA. The detailed attack strategies are described as follows.

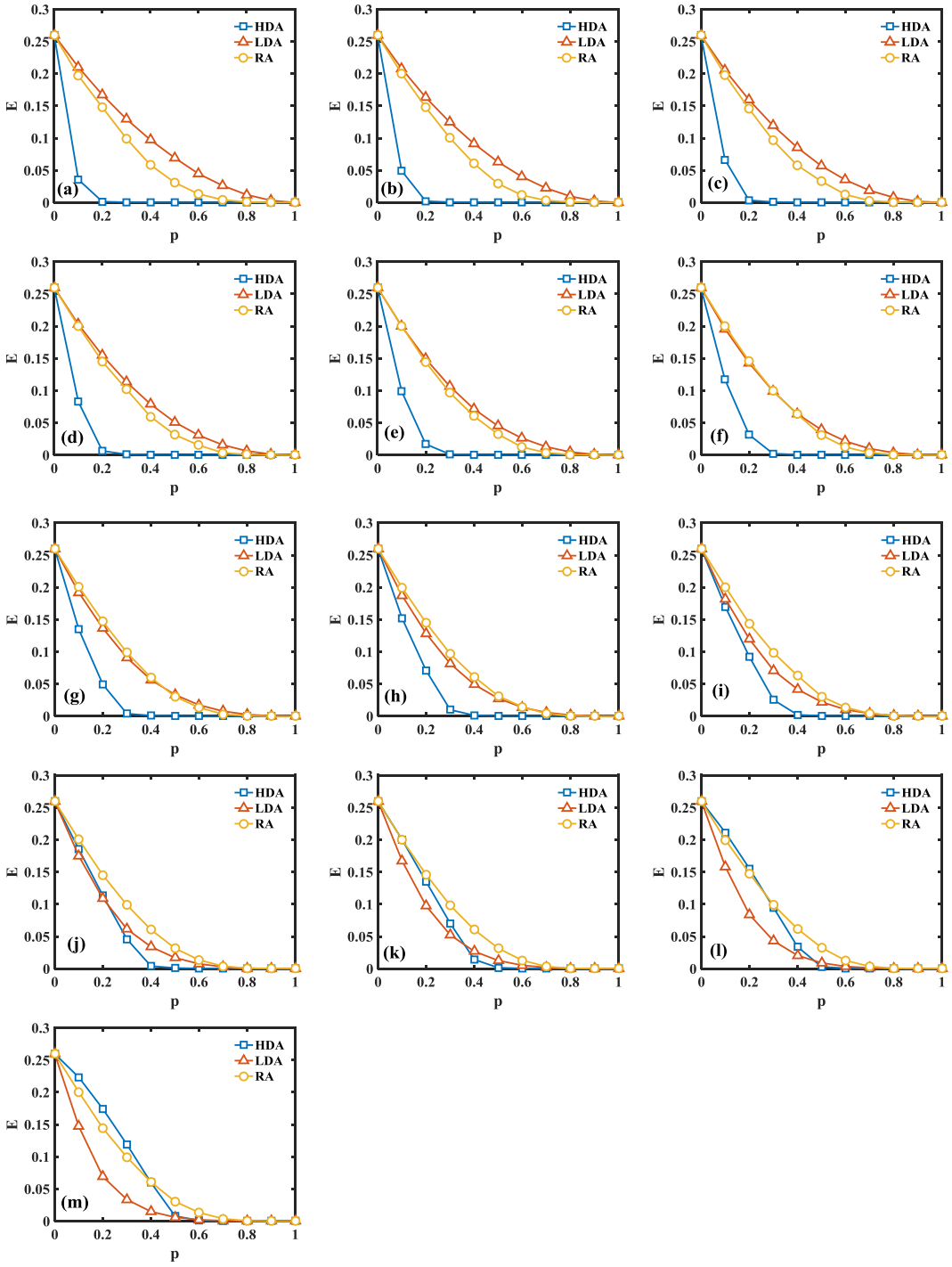

FIGURE 5. The network efficiency E when considering the attack cost. (a) a=0; (b) a=0.1; (c) a=0.2; (d) a=0.3; (e) a=0.4; (f) a=0.5; (g) a=0.6; (h) a=0.7; (i) a=0.8; (j) a=0.9; (k) a=1; (l) a=1.1; (m) a=1.2. BA scale-free network with N=1000 and $\langle k \rangle \approx 4$ is considered. Each point is the average of 10 runs.

1. High-degree attack (HDA) strategy: Sort the nodes in a descending order of their degrees. Then remove the nodes sequentially.

2. Low-degree attack (LDA) strategy: Sort the nodes in an ascending order of their degrees. Then remove the nodes sequentially.

3. Random attack (RA) strategy: Remove the nodes randomly.

It should be noted that our definitions of HDA and LDA are different from those for HDRS and LDRS. In Ref. [15], a node is removed with a probability related to its degree. HDRS defines a higher probability to remove the node with

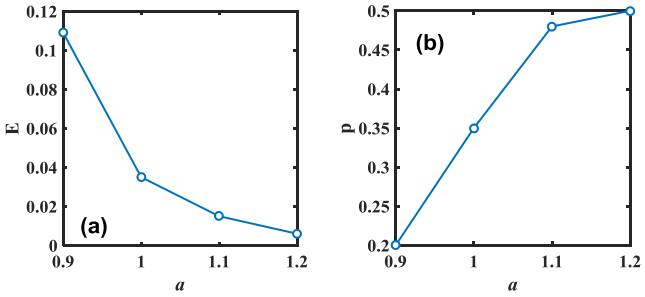

FIGURE 6. The intersection between HDA and LDA curves in figure 5. (a) the network efficiency *E* at the intersection, as a function of *a*. (b) the budget p at the intersection, as a function of *a*. BA scale-free network with N=1000 and $\langle k\rangle \approx 4$ is considered. Each point is the average of 10 runs.

a higher degree, whereas LDRS defines a higher probability to remove the node with a lower degree. In comparison, HDA removes nodes strictly in a descending order of degree, and LDA removes nodes strictly in an ascending order of degree.

In most cases, the attacker has limited budget and can only attack a proportion of nodes, no matter what kind of attack strategy is used. To show the limited budget, we define

$$p = \frac{\sum_{i\in Z} k_i^a}{\sum_{i=1}^{N} k_i^a} \tag{3}$$

where Z is the set of removed nodes. p gives the budget the attacker can use.

C. ROBUSTNESS INDEX

Two indices are considered to show the robustness of networks.

1) THE RELATIVE SIZE OF THE LARGEST CONNECTED COMPONENT

After the attack, the network will be disintegrated into pieces. The largest connected component is the connected piece with the largest number of nodes within it. It shows the best part where the revival nodes can still communicate with each other. So its relative size can be used to measure the robustness of network [22]

$$G = \frac{N'}{N} \tag{4}$$

where N' is the number of nodes in the largest connected component after the attack.

2) NETWORK EFFICIENCY

The efficiency of the network is defined as [23]

$$E = \frac{1}{N(N-1)} \sum_{i\neq j} \frac{1}{d_{ij}} \tag{5}$$

where d_{ij} is the shortest path length between node i and node j.

Compared with the largest connected component, the efficiency takes each and every node into account, instead of those in the largest piece. So this index shows the characteristic of the whole survival network after attack.

III. SIMULATION RESULTS

Figure 1 shows how the relative size of the largest connected component G of the BA network changes with the total attack budget p. It shows that, with higher budget, the attacker always can make more serious damage to the network, no matter what kind of attack strategy is applied.

On the other hand, different attack strategies do have difference. The best attack strategy is always one of the two intentional attack strategies, not RA. Take subfigure (a) as an example. The cost factor a=*0* in this subfigure, which means that the cost to remove different node is the same. Under this condition, it is obviously better to attack the high-degree nodes, which makes the network break quickly. So HDA performs the best among three strategies. On the contrary, if the removal begins from the low-degree nodes, then most of survival nodes are still connected. So LDA performs badly. The performance of RA is between HDA and LDA.

More interestingly, with the change of cost factor a, RA curve almost unchanged, but the performance of intentional attack strategies changes accordingly. Take the last subfigure as an example, where $a = 1$. According to equation (2), the cost to remove a node is proportional to the node's degree when $a = 1$. And we know that the degree distribution of BA network is heterogeneous, which means that a few nodes have a large number of links while most of nodes have only few connections. Thus, the cost to remove a hub is many times higher than the cost to remove a normal node. Then, removal of high-degree nodes may be not a good idea especially when the budget is tight. This is because when the budget is tight, HDA can only remove few hubs, which has litter effect to the whole network. In comparison, LDA can remove a large number of nodes with the same budget. Although each of them is not an important node, the removal of a large number of these unimportant nodes may make the network broken. In the subfigure, when the budget p is low, the LDA curve is the lowest among three curves, followed by the RA curve. Of course, if the budget is higher, HDA still has its advantage. Therefore, in the subfigure, an intersection can be seen between LDA and HDA curves. This intersection is important, since before and after it different attack strategy takes the lead.

Comparing different subfigures in figure 1, the intersection moves. To show it more clearly, we plot how the values of G and p at the intersection change with a in figure 2. It can be seen that both of them are monotone. Since the intersection appears when $a \geq 0.5$ in Fig. 1, the curves in Fig. 2 begin at $a = 0.5$.

Similar results can be seen in ER random graph, as shown in figure 3. And since ER random graph is a homogeneous network, the advantage of HDA is taken over more easily as the intersection appears when a is still small. Figure 4 shows how the values of G and p at the intersection change with a. The results in both networks show that LDA leads HDA for a longer time when the cost gap between removal high-degree node and low-degree node is larger (i.e., when a is larger).

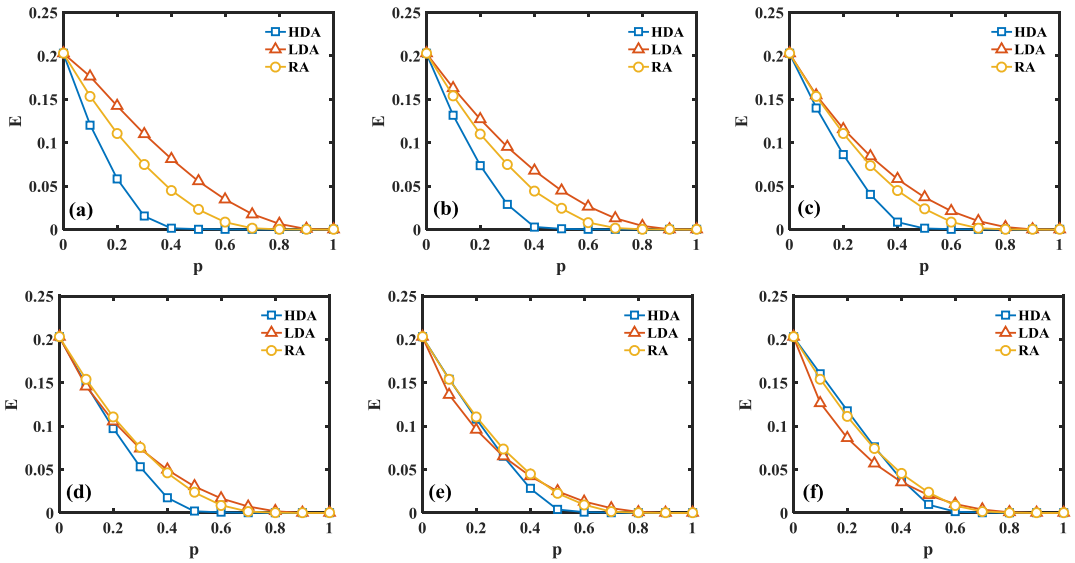

FIGURE 7. The network efficiency E when considering the attack cost. (a) a=0; (b) a=0.2; (c) a=0.4; (d) a=0.6; (e) a=0.8; (f) a=1. ER random graph with N=1000 and $<k>$=4 is considered. Each point is the average of 10 runs.

In the study on network robustness, the largest connected component is often used to measure the performance. However, it only shows the largest connected part of the survival network. To show the whole picture, the network efficiency is a suitable index, as it takes each and every node into account. Figures 5-8 give the network efficiency of BA scale-free network and ER random graph after attack. The intersection between HDA and LDA can be observed in these figures. Comparing to the intersections in figures 1-4, the intersections for the network efficiency appears late. Take the BA scale-free network as an example. The intersection appears when a is greater than 0.5 for the largest connected component (see figure 2), whereas it appears only when a is greater than 0.9 for the network efficiency (see figure 6). During $0.5 < a < 0.9$, HDA seems to be a better attack strategy if the efficiency of the whole network is the key concern, whereas LDA becomes the better strategy if the aim of attack is to reduce the largest connected component. As for RA, the change of a has little impact on the curve.

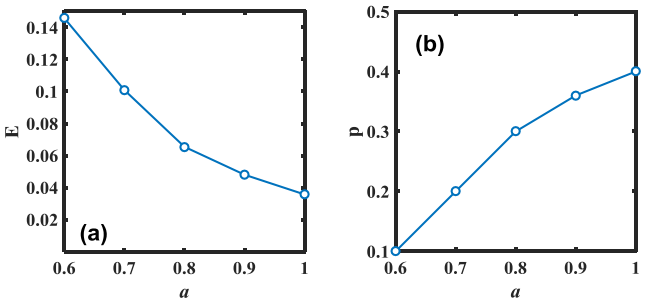

FIGURE 8. The intersection between HDA and LDA curves in figure 7. (a) the network efficiency E at the intersection, as a function of a. (b) the budget p at the intersection, as a function of a. ER random graph with N=1000 and $<k>$=4 is considered. Each point is the average of 10 runs.

IV. CONCLUSION

There are different strategies to attack a complex network. Then the key issue is to find a better one. From the study in this paper, it is shown that the better strategy may change with conditions such as the cost function for the attack, the budget the attacker has, the network structure the attacker is facing, the performance measure the attacker concerns about, and so on. More specifically, when the attack cost is taken into account, attacking the network from the hubs may not be always a good strategy, since hubs cost much higher than most of other nodes. In some cases, attacking unimportant nodes may become a better strategy as it can remove a large number of nodes with the same cost for removing few hubs. In addition, attacking nodes randomly is not a good choice, since there is always one intentional attack strategy better than it. Although this paper is from an attacker's point of view, it is also helpful for the network administrator to defend the network from attacks.

REFERENCES

[1] R. Pastor-Satorras, A. Vázquez, and A. Vespignani, "Dynamical and correlation properties of the Internet," *Phys. Rev. Lett.*, vol. 87, no. 25, Nov. 2001, Art. no. 258701.

[2] B. Li, S. Gao, Y. Liang, Y. Kang, T. Prestby, Y. Gao, and R. Xiao, "Estimation of regional economic development indicator from transportation network analytics," *Sci. Rep.*, vol. 10, no. 1, pp. 581–589, Dec. 2020.

[3] H. Tu, Y. Xia, H. H.-C. Iu, and X. Chen, "Optimal robustness in power grids from a network science perspective," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 66, no. 1, pp. 126–130, Jan. 2019.

[4] Z. Chen, J. Wu, Y. Xia, and X. Zhang, "Robustness of interdependent power grids and communication networks: A complex network perspective," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 65, no. 1, pp. 115–119, Jan. 2018.

[5] W. Yu, T. Wang, Y. Zheng, and J. Chen, "Parameter selection and evaluation of robustness of nanjing metro network based on supernetwork," *IEEE Access*, vol. 7, pp. 70876–70890, May 2019.

[6] Y. Fan, F. Zhang, S. Jiang, C. Gao, Z. Du, Z. Wang, and X. Li, "Dynamic robustness analysis for subway network with spatiotemporal characteristic of passenger flow," *IEEE Access*, vol. 8, pp. 45544–45555, 2020.

[7] H. Zhang, E. Fata, and S. Sundaram, "A notion of robustness in complex networks," *IEEE Trans. Control Netw. Syst.*, vol. 2, no. 3, pp. 310–320, Sep. 2015.
[8] W. Zhang, Y. Xia, B. Ouyang, and L. Jiang, "Effect of network size on robustness of interconnected networks under targeted attack," *Phys. A, Stat. Mech. Appl.*, vol. 435, pp. 80–88, Oct. 2015.
[9] Z. Song, Y. Sun, H. Yan, D. Wu, P. Niu, and X. Wu, "Robustness of smart manufacturing information systems under conditions of resource failure: A complex network perspective," *IEEE Access*, vol. 6, pp. 3731–3738, 2018.
[10] W. Wu, Q. Xu, Z. Liu, and N. Wang, "A probabilistic theory based method for robustness assessment of bipartite networks," *IEEE Access*, vol. 7, pp. 35359–35369, 2019.
[11] V. Carchiolo, M. Grassia, A. Longheu, M. Malgeri, and G. Mangioni, "Network robustness improvement via long-range links," *Comput. Social Netw.*, vol. 6, no. 1, pp. 1–16, Dec. 2019.
[12] Y. Yang, B. Sun, S. Wang, Y. Li, and X. Li, "Controllability robustness against cascading failure for complex logistics networks based on nonlinear load-capacity model," *IEEE Access*, vol. 8, pp. 7993–8003, 2020.
[13] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, Jul. 2000.
[14] B. Zheng, D. Huang, D. Li, G. Chen, and W. Lan, "Some scale-free networks could be robust under selective node attacks," *EPL*, vol. 94, no. 2, p. 28010, Apr. 2011.
[15] C. Hong, X.-B. Cao, W.-B. Du, and J. Zhang, "The effect of attack cost on network robustness," *Phys. Scripta*, vol. 87, no. 5, Apr. 2013, Art. no. 055801.
[16] X. Zhang, G. Xu, and Y. Xia, "Optimal defense resource allocation in scale-free networks," *Phys. A, Stat. Mech. Appl.*, vol. 492, pp. 2198–2204, Feb. 2018.
[17] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, Oct. 1999.
[18] A.-L. Barabási, "Scale-free networks: A decade and beyond," *Science*, vol. 325, no. 5939, pp. 412–413, Jul. 2009.
[19] A.-L. Barabási, R. Albert, and H. Jeong, "Mean-field theory for scale-free random networks," *Phys. A, Stat. Mech. Appl.*, vol. 272, nos. 1–2, pp. 173–187, Oct. 1999.
[20] P. Erdös and A. Rényi, "On random graphs," *Pub. Math., Debrecen*, vol. 6, pp. 290–297, Jan. 1959.
[21] P. Erdos and A. Rényi, "On the evolution of random graphs," *Pub. Math. Inst. Hungarian Acad. Sci.*, vol. 5, no. 1, pp. 17–60, Jan. 1960.
[22] A. E. Motter and Y.-C. Lai, "Cascade-based attacks on complex networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 66, no. 6, Dec. 2002, Art. no. 065102.
[23] P. Crucitti, V. Latora, M. Marchiori, and A. Rapisarda, "Efficiency of scale-free networks: Error and attack tolerance," *Phys. A, Stat. Mech. Appl.*, vol. 320, pp. 622–642, Mar. 2003.

CHENGWANG WANG received the B.Eng. degree in communication engineering from Hangzhou Dianzi University, Hangzhou, China, in 2019, where he is currently pursuing the master's degree. His research interest includes robustness analysis of complex networks.

YONGXIANG XIA (Senior Member, IEEE) received the B.Eng. and Ph.D. degrees in electronic engineering from Tsinghua University, China, in 1998 and 2004, respectively.

He worked with Hong Kong Polytechnic University, Australian National University, and Zhejiang University. He joined Hangzhou Dianzi University, as a Professor, in 2019. His research interests include network science and engineering, including link prediction, network traffic analysis, robustness, and optimization of complex networked systems. He is a member of the IEEE Nonlinear Circuits and Systems Technical Committee and the IEEE Power and Energy Circuits and Systems Technical Committee. He served as the Track Co-Chair for the IEEE 2019 International Symposium on Circuits and Systems (ISCAS 2019). He is an Associate Editor of the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS II: EXPRESS BRIEFS. He is an Editorial Board Member of Scientific Reports.