Vulnerability Analysis for Complex Networks under the Shortest Path-Attack Strategies

Yaohui Hao[1,2,*], Jihong Han[1], Qinghua Cheng[3] and Yongjin Hu[1]
[1] Zhengzhou Institute of Information Science and technology, Zhengzhou 450001, China
[2] State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China
[3]School of Dalian Aeronautics Communication, Dalian 116600, China
[*]Corresponding author

***Abstract*— We proposed three shortest path-attack strategies and investigated the vulnerability of three complex model networks under these path-attack strategies. The experimental results indicate that the robustness of random network is the weakest, but small-world network is the strongest under the shortest path-attack strategies. We also obtain that the shortest path-attack strategies are more harmful than RPA(random augmenting approach) attack strategy. These findings supplement and extend the previous attack results and can thus help us to provide some insights into the design of more robust networks.**

Keywords-vulnerability; complex network; shortest path-attack; degree; betweeness

I. INTRODUCTION

During the past decade, much research has been concerned with issues of the vulnerability of complex networks [1-4]. For example, Albert et al. found that scale-free networks can tolerate very high levels of random failures, but can be disintegrated into small components quickly under malicious attacks[5,6]. Holme et al. proposed four different attack strategies: ID (the initial degree removal), IB (the initial betweenness removal), RD (the recalculated degree removal), and RB (the recalculated betweenness removal), and found that the small-world networks have strong resilience against these four attack strategies[7]. On the basis of these studies, Nie et al. proposed two new attack strategies: IDB (initial degree and betweenness) and RDB (recalculated degree and betweenness), and improved the efficiency of the attack strategies[8], and so on. These studies had drawn many constructive conclusions.

However, when analyzing the vulnerability of the network structure, researchers generally adopted the attack strategy of randomly or intentionally removing a certain percentage of the network nodes or edges. So, Pu found that "terrorists usually prefer much larger scale attacks, and drugs always affect many targets". The RPA(the random augmenting approach) and HPA(the Hamilton path based approach) longest path-attack strategies were proposed on this basis[9]. However, according to the experimental results of Milgram[10], when people choose a path in the network, they tend to choose the shortest one between two points.

As such, we proposed three types of the shortest path-attack strategies and investigated vulnerability of three model networks: random network, scale-free network, small-world model networks. Note that, all the experiments and algorithms are based on the assumption that the networks are undirected and there is only one edge between two nodes.

II. IMPLEMENTATION AND MEASUREMENT

A. Measurement of Damages

In this paper, the efficiency of attack strategies is determined by the relative size of the largest connected component following a fraction of nodes. Here, N is the number of nodes in initial network, LCC the number of nodes in the largest connected component after the attack. To compare the initial networks with different number of nodes, we can execute a data reduction on the network size. The formula is as follows.

$$LCC' = \frac{LCC}{N}$$

$LCC' \in (0,1]$, The size of LCC' reflects the communication capability of a network. When the value of f (remove node ratio) is the same, the larger the largest connected component, the more highly connected the network, it means that the network is highly robust under these attack strategies.

B. Implementation of the Shortest Path-Attacks

In this paper, the shortest path-attacks are implemented iteratively, i.e., each time the nodes of a path are removed until all the nodes in the network are disconnected. In each iteration step of the attacks process, we need to find the shortest path between two nodes in the network.

Floyd and Dijkstra are classical algorithms of the shortest path [11], in this thesis we adopt the Floyd algorithm obtaining the nodes of the shortest path. The specific implementation processes of the shortest path-attacks are shown in Figure I.

To ensure that there is a path between two nodes, we choose the source node and the destination node in the largest connected component of network.

1) Initial condition: Network G with N nodes has $N(N-1)/2$ edges at most, and A is the distance matrix of G. Let a_{ij} be

the flag whether there is an edge between node i and node j, if there is an edge between two nodes, $a_{ij} = 1$, otherwise, $a_{ij} = \infty$ ($i \neq j$, if $i=j$, then $a_{ii} = 0$).

*2) Source and Destination Nodes: I*n the network, different strategies for choosing source and destination nodes lead to different length and nodes of the shortest path, then destructive effect may be different by removing the shortest path. According to the research results of network centrality, the nodes with max degree or max betweenness play an important role in network connectivity[12,13], these nodes are often chosen as the first node to destroy. So, we propose three selecting strategies of source and destination nodes, namely, selecting two max betweeness nodes, selecting two max degree nodes or randomly selecting two nodes.

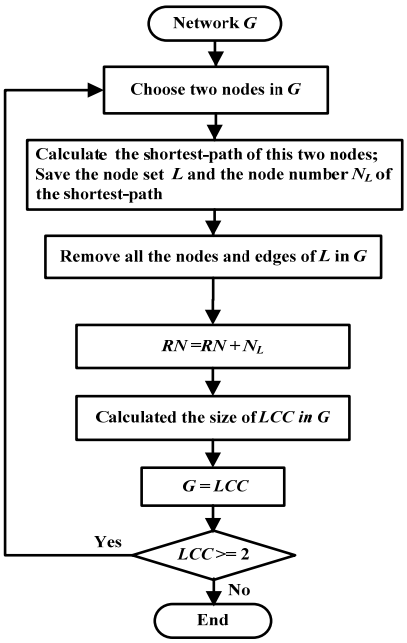

FIGURE I. THE FLOW DIAGRAM OF THE SHORTEST PATH-ATTACKS

Degree of a node *i* is defined by

$$k_i = \sum_{j=1}^{N} a_{ij} = \sum_{j=1}^{N} a_{ji} ,$$

where a_{ij} is the element of the adjacency matrix *A* in the given network *G* and a_{ij} =1.

Analogously, Betweenness of node *i* is defined as the sum of proportions of the number of shortest paths between all pairs of destination nodes that go though node *i:*

$$B_i = \sum_{s \neq i \neq t} \frac{n_{st}^i}{g_{st}} ,$$

where g_{st} is the total number of the shortest paths from node *s* to node *t*, and n_{st}^i is the number of those that pass through the node *i*. In a network, Betweenness counts the number of geodesic paths that pass through a node.

3) Nodes of the shortest path: In this paper, we propose three shortest path-attack strategies based on three different selecting strategies of source and destination nodes. The descriptions are as follows:

a) RSP(the shortest path between random two nodes): First, RSP randomly selects two nodes in the network as source and destination nodes. Second, RSP calculates the shortest path between these two nodes and saves the nodes of the shortest path.

b) BSP(the shortest path between two nodes with the max betweeness): First, BSP sorts the nodes according to betweeness in descending order. Second, BSP selects two max betweeness nodes as source and destination nodes. Third, BSP calculates the shortest path between these two nodes and saves the nodes of the shortest path.

c) DSP(the shortest path between two nodes with the max degree): DSP adopts a similar method as (2), but the difference is that DSP selects the source and destination nodes with the max degree.

4) Iterative operation: Each iteration indicates implementing of a shortest path-attack, this means that each node *i* in shortest path would be removed from the network. For the distance matrix *A*, set all the elements in row *i* and column *i* of the distance matrix *A* to be *zero*.

5) Termination criterion: When the size of the largest connected component in the current network *G* is 1, which means all the nodes in *G* are isolated, the iteration will then be terminated.

III. NUMERICAL RESULTS AND ANALYSIS

In this section, the proposed three shortest path-attack strategies and RPA [9] are applied to random, scale-free and small-world three model networks. The results of RSP and RPA are the average of 1000 independent runs.

A. Model Networks

Firstly, we study the change of the largest connected component *LCC'* for random, scale-free and small-world model networks, under three different shortest path-attack strategies and one approximate longest-path-attack strategies. The fluctuation curves of *LCC'* are shown in Figure II.

Figure II shows that the random network behaves similar to the small-world network in the process of these five attack strategies while the scale-free network behaves much differently.

For the random network (Figure II (a)), the relative size of the giant component decays linearly and the *LCC'* is almost same in the range $0 < f < 0.4$ for all the attack strategies. It is distinct that the efficiency of these four attack strategies is

almost the same at the beginning of attacks. When f >0.4, for a given f, *LCC'* has a relationship as follow: $LCC(f)_{RPA} > LCC(f)_{RSP} > LCC(f)_{DSP} \geq LCC(f)_{BSP}$, it is distinct that the efficiency of attack strategies is BSP ≥ DSP > RSP > RPA. And, for BSP and DSP, the random network reaches to the threshold f_c only when approximately 50% fraction of vertices is removed, for RPA, the fraction of vertices is 91%. So, the attack efficiency of BSP and DSP is improved by about 33% compared with RPA strategy.

For small-world network (Figure II (c)), the fluctuation curves of *LCC'* are similar to random network, at the beginning of attacks, *LCC'* is almost the same for five the attack strategies, differently, when f >0.53, the decrease of *LCC'* is different.

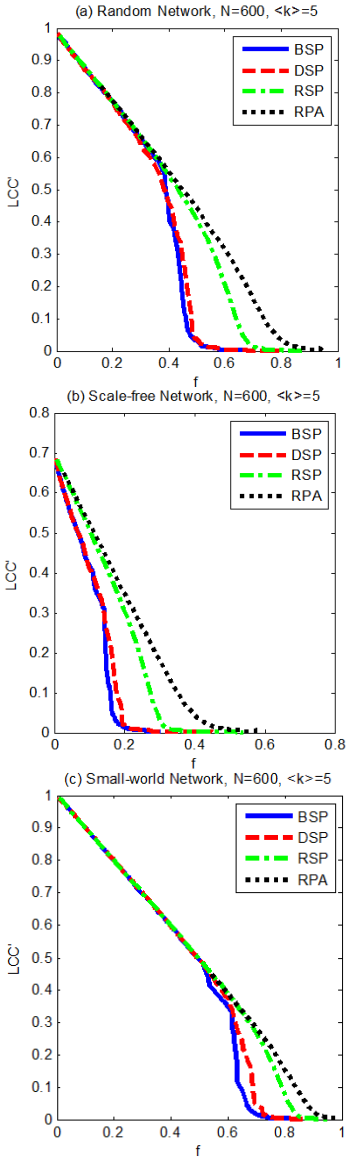

FIGURE II. THE VARIATION OF *LCC* UNDER DIFFERENT ATTACK STRATEGIES

But, for the scale-free network (Figure II (b)), at the beginning of the attacks, the largest connected component of BSP and DSP decays faster than that of other attack strategies. For a given f, LCC' has a relationship as follow: LCC(f)RPA > LCC(f)RSP > LCC(f)DSP ≥ LCC(f)BSP, it is distinct that the efficiency of attack strategies as BSP ≥ DSP > RSP > RPA.

Moreover, for these three model networks, we can see two crosses between BSP and DSP path-attack strategies in Figure II (a)(b)(c). Within a certain range, nodes are removed (0.38≤ f ≤ 0.47 in Figure II (a) , 0.15 ≤ f ≤ 0.20 in Figure II (b) and 0.5 ≤ f ≤ 0.75 in Figure II (c)), BSP can perform more destructive effect than DSP, in other cases, the efficiencies of BSP and DSP attack strategies are almost the same.

Overall, the three shortest path-attack strategies behave more efficiently than RPA the longest path-attack strategies for these three model networks.

Then, we compare changes of the largest connected components of random, scale-free and small-world model networks under three shortest path-attack strategies, as shown in Figure III.

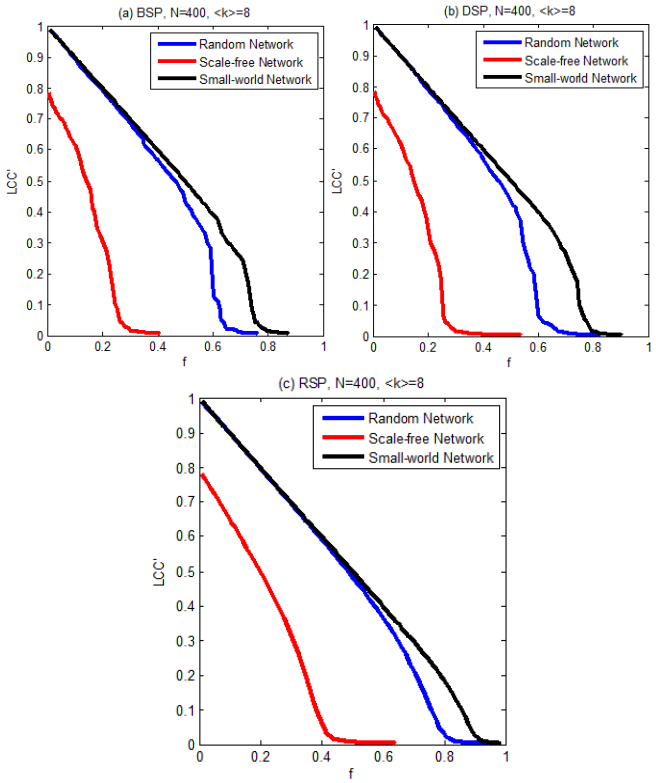

FIGURE III. THE VARIATION OF LCC UNDER DIFFERENT MODEL NETWORKS

In Figure III (a)(b)(c), the fc of scale-free is the smallest, and for a given f, the LCC' of scale-free the lowest. It can be concluded that the robustness of scale-free network is the weakest under these shortest path-attack strategies.

For random network and small-world network, at the beginning of the shortest path-attacks, the fluctuation curves of *LCC'* is almost the same, but as the removed nodes increase, there is the branch for scale-free and small-world model

networks under these three shortest path-attack strategies. Moreover, the curves of random model network declines most rapidly, but the curves of small-world model network declines most slowly. It can be concluded that the robustness of the small-world network is the strongest in three model networks under these shortest path-attack strategies.

In addition, we calculate the average path length of random, scale-free and small-world model networks when N=400 and $\langle k \rangle$=8, as seen from Table I.

TABLE I. THE AVERAGE PATH LENGTH OF MODEL NETWORKS

<k>	**The Average Path Length**		
	Random	***Scale-free***	***Small-world***
8	3.1518	2.3126	2.2251

From Table I, it is clear that the average path length of small-world network is the lowest. So, the shortest path-attack strategies are less efficient for small-world network.

IV. CONCLUSIONS

In this study, we analyze the vulnerability of three model networks by iteratively implementing three different shortest path-attack strategies named BSP(the shortest path between two nodes with the max betweeness), DSP(the shortest path between two nodes with the max Degree) and RSP(the shortest path between random two nodes). Comparing the efficiency of the three path-attacks, the experimental results indicate that the robustness of random network is the weakest, but small-world network the strongest under these the shortest path-attack strategies. Furthermore, we also obtain that the shortest path-attack strategies are more harmful than RPA (the approximate longest-path-attack strategy). These findings can help us better explaining the robustness of different networks under different new attack strategies, while providing some insights into the design of high survivability networks.

ACKNOWLEDGMENT

We thank Dr. Hong Guo for many discussions and fruitful exchanges.

REFERENCES

[1] B.P. Duan, J. Liu, M.X. Zhou, L.L. Ma, “comparative analysis of network robustness against different link attacks”, Physica A, vol.448, 2016, pp.144-153.

[2] H.P. Ren, J. Song, R. Yang, M.S. Baptista, C. Grebogi, “Cascade failure analysis of power grid using new load distribution law and node removal rule”, Physica A, vol.442, 2016, pp.239-251.

[3] M. Bellingeri, D. Cassi, S. Vincenzi, “Efficiency of attack strategies on complex model and real-world networks”, Physica A, vol.414, 2014, pp.174-180.

[4] A. Yehezkel, R. Cohen, “Degree-based attacks and defense strategies in complex networks”, Physical Review E, vol.86, 2012:066114.

[5] R. Albert, H. Jeong, A. L. Barabasi, “Internet: Diameter of the World-Wide-Web”, Nature, vol.401, 1999, pp.307-309.

[6] R. Albert, H. Jeong, A. L. “Barabasi, Error and attack tolerance of complex networks”, Nature, vol.406, 2000, pp.387-482.

[7] P. Holme, B. J. Kim, C. N. Yoon, S. K. Han, “Attack vulnerability of complex networks”, Physical Review E, vol.65, 2002: 056109.

[8] T. Y. Nie, Z. Guo, K. Zhao, Z.M. Lu, “New attack strategies for complex networks”, Physica A, vol.424, 2015, pp.248-253.

[9] C.L.Pu, W. Cui, “Vulnerability of complex networks under path-based attacks”, Physica A, vol.419, 2015, pp.622-629.

[10] S. Milgram, “The Small World Problem”, Psychology Today, vol.2, 1967, pp.185-195

[11] A. Naomichi, W. Yoshihide, I. Toshiaki, “Implementation of the network simplex algorithm to MATLAB by way of the shortest path problem”, Science & Engineering Review of Doshisha University, vol. 52, 2011, pp.99-106.

[12] J. W. Wang, L. L. Rong, “Cascade-based attack vulnerability on the US power grid”, Safety Science, vol. 47, 2009, pp.1331-1336.

[13] J. Hendler, N. Shadbolt, W. Hall, T. Berners-Lee, D. Weitzner, “Web science: an interdisciplinary approach to understanding the web”, Communications of the ACM, vol.51, 2008, pp.60-69.