Evaluation and optimization of complex network resilience against attacks

Qi Xiaogang*, Zhang Biwen, Liu Lifang, Hu Shaolin

School of Mathematics and Statistics, Xidian University, Xi'an, 710071, China
*corresponding author's email: xgqi@xidian.edu.cn

***Abstract*—With the current communication network failures intensifying, they have characteristics of complexity and adaptability. This is no longer possible that networks can completely resist all kinds of network attacks. Targeted attacks and random failures may cause link or node removal, which in turn can cause significant disruption to the availability of network services. Designing a network topology to provide acceptable levels of service in the face of these challenges can prolong the network lifetime. In this paper, an iteration algorithm called average efficiency improved (AE-improved) algorithm is presented to improve the given robustness functions. The algorithm improves the topology resilience of three complex networks by adding a set of links to maximize the average efficiency of a network. Then, non-improved and improved graphs are evaluated by applying random failure and centrality-based attacks to examine their resilience. The results show that compared with other optimization algorithms, the AE-improved algorithm we proposed yields the best network resilience against such attacks among the studied robustness metrics.**

Keywords- Graph Robustness; Network Resilience; Random Failures; Targeted Attacks; Network Topology

I. INTRODUCTION

Computer network applications are playing a more and more crucial role in supporting kinds of services in the fields such as politics, economy, military and culture. However as an open system, networks suffer from a variety of attacks, failures and the interference and damage of accidents, such as earthquakes, hurricanes, and other natural disasters. The definition of computer network resilience is the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operations [1]. Because those service networks are vulnerable to attacks and natural disasters which can disrupt the normal operation and service delivery [2], it is necessary for network designer to build a network with higher resilience while to provide an acceptable level of service when there are various challenges [3].

To study resilience network structure, previous research has presented a method to design a network model in which they used the constraint of minimum average distance [4]. Kang Zhao and his colleagues presented a hybrid network growth model called degree and locality-based attachment (DLA) model [5]. However, there have been a lot of researches working on network topology optimization, which were used to improve the existing real-world graphs. There are real-world service provider network topologies, such as Sprint, AT&T, GÉANT2 and so on [6]. Except for classic graph metrics, some graph spectral metrics are used to measure robustness before and after removing nodes or links [7]. Algebraic connectivity, spectral gap [8], natural connectivity [9], weighted spectrum and network criticality have been studied [10]. Different from aforementioned researches, this paper proposes an iterative algorithm to optimize existing network topologies and to improve the network capacity in the absorption of damage.

Our contribution in this work is threefold. First, we introduce an optimization algorithm to improve a given graph based on the average efficiency function. Second, the proposed AE-improved algorithm is applied to three complex networks and generate improved graphs. Third, we apply the flow robustness function on improved graphs to evaluate the resilience of these networks against random failures and malicious attacks.

II. RELATED WORK

In this section we introduce graph theoretic background and related work to network robustness metrics.

A. Graph centrality metrics

A complex network can be viewed as a simple undirected graph $G=(V,E)$, where V is the set of nodes and E is the set of links. Centrality metrics measure the importance of a node or a link in a network. Due to the importance of a node or a link varies in different applications, central nodes based on the given application should be identified.

The node degree $D(v)$ can be considered as the importance of node connectivity. The node degree is a kind of local centricity metric, because it only depends on the number of links connected locally. The node betweenness $B(v)$ is the number of the shortest paths through the node v. Betweenness is a global variable and reflects the influence of the corresponding node or link in the entire network. Closeness $C(v)$ is a centrality metric that measure the average distance between node v and other nodes in the network.

B. Related graph spectral theory

Spectral graph theory investigates the relationship between graphs structure and eigenvalues and eigenvectors of their adjacency matrices, incidence matrices, and Laplacian matrices [7].

For a given graph $G=(V,E)$, the number of nodes is N and the number of links is K. The adjacency matrix of graph G is $A=(A_{ij})_{N\times N}$, where

$$A_{ij}=\begin{cases}1, & if\ v_i,v_j\ are\ adjacent\\ 0, & otherwise\end{cases} \quad (1)$$

978-1-5386-2813-3/17 $31.00 © 2017 IEEE
DOI 10.1109/ICSGEA.2017.67

The eigenvalue μ is the root of characteristic polynomial. The set of eigenvalues of the adjacency matrix is $\{\mu_1, \mu_2, \ldots, \mu_N\}$, which is a non-decreasing list. Spectral gap $\Delta\mu = \mu_N - \mu_{N-1}$ defined as the difference of two eigenvalues, where μ_N is the largest and μ_{N-1} is the second largest eigenvalues of the adjacency matrix. Spectral gap is a graph spectral metric measured graph robustness against targeted attacks. Natural connectivity $\bar{\mu}$ defined as $\bar{\mu} = \ln\left[\frac{1}{n}\sum_{i=1}^{N} e^{\mu_i}\right]$, where μ_i is the ith eigenvalue of the adjacency matrix. The larger the natural connectivity value $\bar{\mu}$ is, the greater robustness the graph has. It has been shown that natural connectivity has greatly improved in terms of accuracy and reasonability than average node degree when describing network resilience.

III. NETWORK RESILIENCE OPTIMISATION ALGORITHM

A. Network model

A network can be represented as a graph $G = (V, E)$ with N nodes and K links. Let $V = \{v_1, v_2, \ldots, v_N\}$ represents a set of nodes, $e_{ij} \in E$ represents the link between the node pair $v_i, v_j \in V$. The adjacency matrix is $A = (A_{ij})_{N \times N}$. We assume that two nodes in graph communicate with each other using the shortest path. We use ε_{ij} to denote the efficiency between nodes v_i and v_j, whose definition is the inverse of the shortest distance, i.e. $\varepsilon_{ij} = (1/d_{ij})$, where d_{ij} is the distance between node v_i and v_j. When there is no path between nodes v_i and v_j, then $d_{ij} = +\infty$ and $\varepsilon_{ij} = 0$ correspondingly. Therefore, the definition of the average efficiency of a network is the average of sums of the inverse of the shortest distance between any two nodes in the graph. The value of the average efficiency of a network is calculated as follows:

$$E(G) = \frac{1}{N(N-1)} \sum_{i \neq j \in G} \varepsilon_{ij} \qquad (2)$$

This metric can be used to measure the efficiency or performance of graph G.

B. Optimization Algorithm

In this paper, we present an iteration algorithm called average efficiency improved (AE-improved) algorithm adding a set of links to a given graph. It can be considered as an optimization problem to improve network resilience.

There are two inputs about this topology optimization algorithm: an input graph A_i and the number of links required L_r. For an input graph A_i, the number of nodes and links is N_i and K_i respectively. The number of links required L_r is the number of links added to the graph. In order to record the link selected in each step, the algorithm adds the link to the *selectedLinks* list. At each iteration, the algorithm starts from the graph got in previous iteration. There are three main functions about this topology optimization algorithm: $efficience(G)$, $candidate(G)$ and $improvedLink(L)$. The average efficiency function $efficience(G)$ is the objective function of the algorithm. The candidate function $candidate(G)$ takes a graph G as input. It returns the set of candidate links. Finally, $improvedLink(L)$ function is used to select the link with the highest improvement value, and then add it to the *selectedLinks* list. The algorithm repeats this process until enough links are selected. The pseudocode of our algorithm is shown in Figure 1.

AE-Improvement Algorithm

Function:
$efficience(G)$: =average efficiency function
$candidate(G)$: =candidate links function
$improvedLink(L)$: = the value improved by the link in list L
Input:
A_i : = input graph
L_r : = the number of links required
Output:
G : = improved graph
selectedLinks : = a list of links we selected
Begin
  selectedLinks = [ ]
  iterationList = [ ]
  While *selectedLinks.length*() < L_r **do**
    $G = A_i$
    $G.addlinks(selectedLinks)$
    for $l \in candidate(G)$ **do**
      $improvement = efficience(G, l)$
      $iterationList.append(l)$
    end
    selectedLink =
    $improvedLink(iterationList)$
    $selectedLinks.add(selectedLink)$
  end
  return *selectedLinks*
  return G
end

Figure 1. AE-improved Algorithm

IV. RESILIENCE MEASUREMENT

In this section, we introduce that how flow robustness measures network resilience. Then we present the attack models and three complex network topologies we studied.

Furthermore, we use the flow robustness metric to evaluate network resilience against nodes removal [11].

A. *Flow Robustness*

The definition of flow robustness is the number of reliable flows divided by the number of total flows in the whole network [12]. A flow is defined reliable if there is at least one of its paths unbroken when the link or node failures. For a given graph $G=(V,E)$, $\{C_i;1<i<k\}$ represents the set of components in the entire graph G. The flow robustness of graph G can be calculated as follows:

$$FR(G)=\frac{\sum_{i=1}^{k}|C_i|(|C_i|-1)}{|V|(|V|-1)},\quad 0\le FR\le 1 \qquad (3)$$

The computational complexity depends on the complexity to find components in the graph, which is $O(|V|+|E|)$. Therefore, the algorithmic complexity to calculate flow robustness of graph G is $O(|V|+|E|)$.

B. *Network Attack Models*

In this paper, graph models was used to attack graphs. We use random failure and three centrality-based measures: node betweenness, closeness and degree. For each challenge, we removed the node with the highest centrality [13].

C. *Complex Networks*

In this paper, three topology models were used to measure the availability of the presented algorithm. It included typical complex networks, such as the ER random network model, the BA scale-free network model, and a topology generated model denoted as AD connected networks. In addition, we listed some classic graph metrics of each topology, and provided an insight of the graph properties as shown in Table 1.

Table 1. Three Complex Networks

	Nodes	Links	Avg. Degree	Avg. Hop
ER Network	50	110	4.40	2.74
BA Network	75	210	5.60	2.56
AD Network	50	100	4.00	2.91

V. EXPERIMENTAL RESULTS

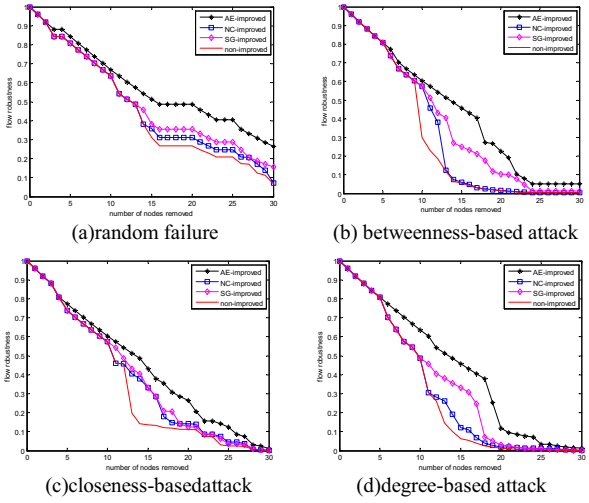
In this paper, we operated the algorithm presented previous, and added links to three complex networks. The number of links we added was the same as the number of nodes in the given network. For each network topology, values of the average efficiency function about non-improved graphs and improved graphs were shown in the third and fourth columns of Table 2 respectively.

Table 2. Average Efficiency of Graphs

	L_r	non-improved AE	improved AE
ER Network	50	0.428	0.682
BA Network	75	0.439	0.689
AD Network	50	0.407	0.656

For the algorithm we presented which took the average efficiency function as the optimization objective function, we compared it with two kinds of optimization algorithms, and observed the effects the algorithm improved. One was a natural connectivity improvement algorithm. Another was a spectral gap improvement algorithm.

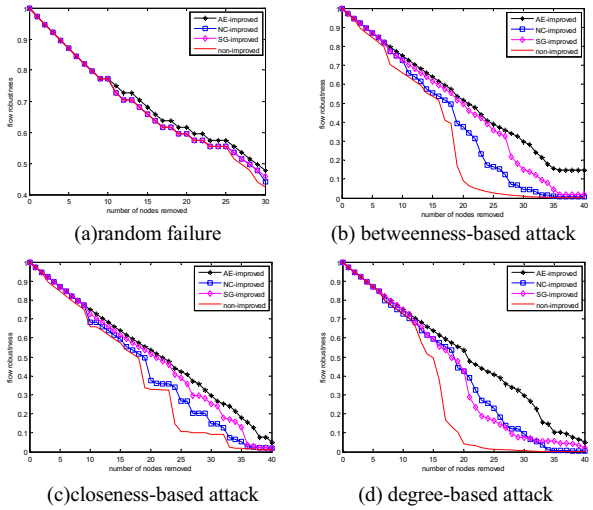
For each network model, we input an initial graph, and got three improved graphs generated by the algorithm presented and two contrasting algorithms, denoted as non-improved, AE-improved, NC-improved, and SG-improved networks. The results of applying the graph random failure and three centrality attacks to non-improved, AE-improved, NC-improved, and SG-improved graphs were shown in Figure 2, 3, and 4. Network robustness of ER random graphs under random failure was shown in Figure 2(a). The flow robustness of AE-improved graphs against node attacks were expressed as the black curves with asterisks. The blue curves, magenta curves, and red curves showed the flow robustness of NC-improves, SG-improved, and non-improved graphs respectively. The results of network resilience under node betweenness attack, closeness attack, and degree attack are shown in Figure 2(b), 2(c), and 2(d). Among the three improved graphs analyses, the conclusion was that the AE-improved graphs are more resilient than the NC-improved and SG-improved graphs against node attacks. The finding hold up even after we adjusted for other network models, such as BA scale-free and AD connected network models as shown in Figure 3 and Figure 4. The black curves indicating the improved algorithm of the average efficiency function were above other curves, and had the highest value than others. We used the flow robustness metric to quantify network resilience. The larger the value was, the more resilient the network was. By studying the results for all networks presented in Table 2, we observed that AE-improved algorithms shows the highest consistency among robustness algorithms we studied in providing the best network resilience against random failure and centrality-based attacks.



(a)random failure (b) betweenness-based attack

(c)closeness-basedattack (d)degree-based attack

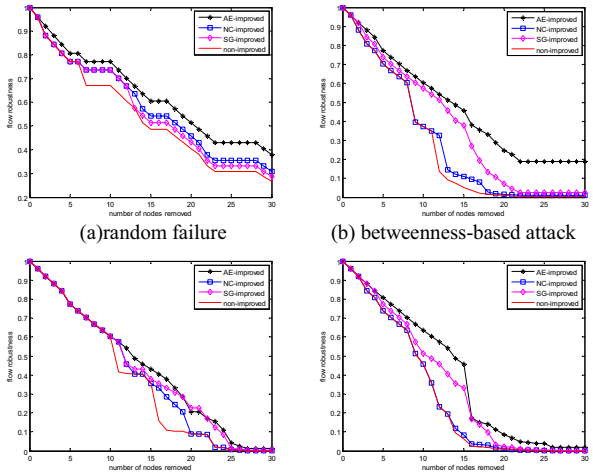
Figure 2. Flow Robustness Analysis of ER Random Network



(a)random failure (b) betweenness-based attack

(c)closeness-based attack (d) degree-based attack

Figure 3. Flow Robustness Analysis of BA Scale-free Network



(a)random failure (b) betweenness-based attack

(c)closeness-based attack (d) degree-based attack

Figure 4. Flow Robustness Analysis of AD connected Network

VI. CONCLUSIONS

Evaluating and improving communication networks resilience when random failures and targeted attacks existed is an important aspect of network security. In this paper, an iterative algorithm was presented to optimize the network topology and improve resilience. The algorithm was applied on three complex networks, then generated some improved graphs and compared the utility of this algorithm. Using the flow robustness graph metric, non-improved and improved graphs were evaluated by applying random failures and centrality-based attacks to examine their resilience. The results show that average-efficiency-improved graphs are more resilient against random failures and targeted attacks than both graphs generated by adding links to improve the natural connectivity and spectral gap metrics of the network. The further work is to investigate how to generate the most resilient topology, while minimizing cost if we consider the capacity of a node or link.

ACKNOWLEDGEMENTS

This work is supported by Natural Science Foundation of China (Grants Nos. 61572435, 61472305, 61473222); the Natural Science Foundation of Shaanxi Province (Grant Nos. 2015JZ002, 2015JM6311); the Natural Science Foundation of Zhejiang Province(Grant No. LZ16F020001); Programs Supported by Ningbo Natural Science Foundation (Grant No. 2016A610035).

REFERENCES

[1] J. P. G. Sterbenz, D. Hutchison, E. K. Cetinkaya. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. Computer Networks, 2010, 54(8): 1245–1265.

[2] X. Long, D. Tipper, T. Gomes. Measuring the survivability of networks to geographic correlated failures. Optical Switching and Networking, 2014, 14(2): 117–133.

[3] J. P. G. Sterbenz, E. K. Cetinkaya, M. A. Hameed. Evaluation of Network Resilience, Survivability, and Disruption Tolerance: Analysis, Topology Generation, Simulation, and Experimentation (invited paper). Telecommunication Systems, 2013, 52(2): 705–736.

[4] Y. J. Li, Y. F. Peng, S. Du. Survivability Optimization and Analysis of Network Topology Based on Average Distance. SPIE-OSA-IEEE Asia Communications and Photonics, 2009, 7633: 76331N-1- 6.

[5] K. Zhao, A. Kumar. Analyzing the Resilience of Complex Supply Network Topology Aginst Random and Targeted Disruptions. IEEE SYSTEMS JOURNAL, 2011,5(1): 28-39.

[6] M. J. F. Alenazi, J. P. G. Sterbenz. Comprehensive comparison and accuracy of graph metrics in predicting network resilience. 2015 /11th International Conference on the Design of Reliable Communication Networks (DRCN 2015), 2015.

[7] M. J. F. Alenazi, J. P. G. Sterbenz. Evaluation and Comparison of Several Graph Robustness Metrics to Improve Network Resilience. IEEE, 2015: 7-13.

[8] J. Wu, M. Barahona. Spectral Measure of Structural Robustness in Complex Networks. IEEE TRANSACTIONS ON SYSTEMS, 2011, 41(6): 1244-1252.

[9] Jun Wu, Suoyi Tan, Yuejin Tan, Hongzhong Deng. Analysis of Invulnerability in Complex Networks Based on Natural Connectivity. COMPLEX SYSTEMS AND COMPLEXITY SCIENCE, 2014, 11(1): 77-86. (in Chinese)

[10] D. Fay, H. Haddadi. Weight Spectral Distribution for Internet Topology Analysis: Theory and Applications. IEEE/ACM TRANSACTIONS ON NETWORKING, 2009, 18(1): 164-176.

[11] M. J. F. Alenazi, J. P. G. Sterbenz. Evaluation and Improvement of Network Resilience against Attacks using Graph Spectral Metrics. IEEE, 2015: 206–211.

[12] E. K. Cetinkaya, A. M. Peck, J. P. G. Sterbenz. Flow Robustness of Multilevel Networks. 274- 281.

[13] P. Y. Chen, A. O. Hero. Assessing and Safeguarding Network Resilience to Nodal Attacks. IEEE Communications Magazine, 2014: 138- 143.