Measuring Topological Robustness of Scale-Free Networks Using Biconnected Components

Suri Dipannita Sayeed, Md. Sajid Hasan, Md. Saidur Rahman
Department of Computer Science and Engineering
Bangladesh University of Engineering and Technology (BUET)
Dhaka-1000, Bangladesh
Email: suri.esha6@gmail.com, sajid.cse.08@gmail.com, saidurrahman@cse.buet.ac.bd

***Abstract*—Models of complex networks are dependent on various properties of networks like connectivity, accessibility, efficiency, robustness, degree distribution etc. Network robustness is a parameter that reflects attack tolerance of a network in terms of connectivity. In this paper we have tried to measure the robustness of a network in such a way that gives a better idea of both stability and reliability of a network. In some previous works, the existence of a giant connected component is considered as an indicator of structural robustness of the entire system. In this paper we show that the size of a largest biconnected component can be a better parameter for measurement of robustness of a complex network. Our experimental study exhibits that scale-free networks are more vulnerable to sustained targeted attacks and more resilient to random failures.**

I. Introduction

Study and research on complex networks has become an attractive and dominant field over the last couple of years. Two well known and much studied classes of complex networks are scale-free networks and random networks. A scale-free network is a network whose degree distribution follows a power law distribution $P(k) = k^{-\gamma}$ with an exponent γ that ranges between 2 and 3. A random graph is a graph that is generated by some random process. In our paper, we are trying to measure robustness of scale-free networks.

Network robustness is a measurement of sustainability, attack tolerance or error recovery of a network. It is an intuitive idea. It is considered from two perspective, one is attack and the other is failure. In case of attack, a network aims at disrupting quickly, like any biological network attacked by any malicious virous. Failure on the other hand aims at slow disintegration, like a router network. In both cases measuring robustness is important. Most real-world networks have heterogeneous degree distributions (i.e. they have a large number of nodes with small degree, a small number of nodes with high degree), hence studying the robustness of scale-free networks seems relevant.

Many researches have been made on this topic. Previously derived methods of measuring robustness of a network involved various different parameters and approaches. Previous researchers used parameters like diameter, size of the largest connected component of network, average size of the rest of the network, degree, betweenness etc, for analyzing a network. Albert et al. [1] researched on two fundamental network construction types i.e. Erdös and Rényi (ER) model and the scale-free model. They showed that a huge network with a small diameter means its nodes are well connected i.e. there are a lot of alternative paths between the nodes. During random attack, in the case of random network, the diameter increased with the increased amount of nodes removed. In case of a scale free network, the diameter remained unchanged. A targeted attack on the other hand, shows different results. The effect on the random network is almost the same but for the scale free network the diameter increased rapidly. They also analyzed the size of the largest component S and the average size s of the components other than the largest component. They found that S and s both shows a threshold like behavior. In case of random failure, the largest component size decreases gradually with increasing number of nodes removed. For targeted attack, the component size falls drastically. Crucitti et al. [2] researched on network robustness using three different factors i.e. degree, betweenness and an improvement on betweenness in which the shortest paths were recalculated each time a vertex was removed. They calculated network robustness as "global efficiency" which is the average of efficiency between each pair of vertices. Efficiency is the inverse of shortest path length. This measure was actually first adopted by Vito Latora and Massimo Marchiori. Piraveenam et al. [3] introduced robustness coefficient to measure the numerical value of robustness of a network.

In this paper we have tried to measure the robustness of a network in a way that gives more information about the reliability of the network. Our approach is to use the size of the largest biconnected component for the measurement of robustness of the network. We have shown that size of the largest biconnected component in addition with the size of the other connected components give a more reliable robustness coefficient value. Using this coefficient value we have also shown that scale free networks are much more vulnerable towards targeted attacks and resilient towards random attacks.

The rest of the paper is organized as follows. In Section II we discuss the relevant ideas and necessary definitions from graph theory and algorithm theory. Here, we have discussed about connectivity of a network, perturbations in a complex network, existing approaches to measure network robustness etc. Section III contains detail about our research that is biconnectivity as a better approach for measuring network robustness. Section IV contains results of our research and discussion. Finally, we conclude in Section V with some future directions.

978-1-4799-8126-7/15/$31.00

II. PRELIMINARIES

In this section, we discuss some basic concepts of graph theory related to networks such as connectivity of a network, perturbations in a complex network, existing approaches to measure network robustness etc.

A. Terms and definitions

Let, G=(V, E) be a graph with a set V of vertices and a set E of edges. A v_0, v_l-*path*, $v_0, e_1, v_1, \ldots, v_{l-1}, e_l, v_l$, in G is an alternating sequence of distinct vertices (except possibly v_0, v_l) and edges of G, beginning and ending with a vertex such that each edge is incident to the two vertices immediately preceding and following it. A path or walk is *closed* if $v_0 = v_l$. A closed path containing at least one edge is called a *cycle*. A graph G is a *connected graph* if for every pair $\{u, v\}$ of distinct vertices there is a path between u and v. A connected graph without a cycle is a tree. A graph which is not connected is called a *disconnected graph*. A *connected component* of a graph G is a maximal connected subgraph of G. A *biconnected component* of an undirected graph is a maximal subgraph in which at least 2 vertices have to be deleted to make the subgraph fragmented. Such subgraphs are sometimes called blocks or nonseparable subgraphs. A simple graph in which each pair of distinct vertices are adjacent is a complete graph. If the graph representing a network is a complete graph, then the network is termed as an *ideal network*. If graph G has a u, v path, then the distance from u to v written $d_G(u, v)$ or simply $d(u, v)$, is the length of a shortest u, v path. The diameter is $max_{u,v \epsilon_V} d(u, v)$.

Robustness is the property of a network which denotes the attack tolerance of that network. It measures the extent to which it is difficult to cut the network into independent components. Network structure has high influence on robustness of a network. Robustness increases with the increase of connectivity of a network. *Strictly robust network* is a network that contains alternate paths between each pair of vertices. As long as a maximal biconnected subgraph exists in the network, it is considered as strictly robust. The minimum connectivity which makes a graph strictly robust is biconnectivity. Strict robustness increases with the increase of connectivity in the network.

Connectivity of network plays a significant role in determining network robustness. To quantify connectivity, analysts use two concepts.

- *Edge Connectivity:* The minimum number of edges that have to be removed to disconnect the network. A bridge is an edge whose removal disconnects a graph.
- *Node Connectivity:* The minimum number of nodes that have to be removed to disconnect the network.

The simplest graph theoretical concept that can be used as a measure of *connectivity* is the *density* of the network. A very dense network is generally considered to be well connected. Another aspect of *connectivity* is *reachability*. A network is reachable if all the nodes in the network are accessible to each other. High density normally implies high reachability. However, it is possible to have networks with both high density and low reachability if there is a high level of clustering, i.e. the links are distributed only within, and never between, isolated clusters.

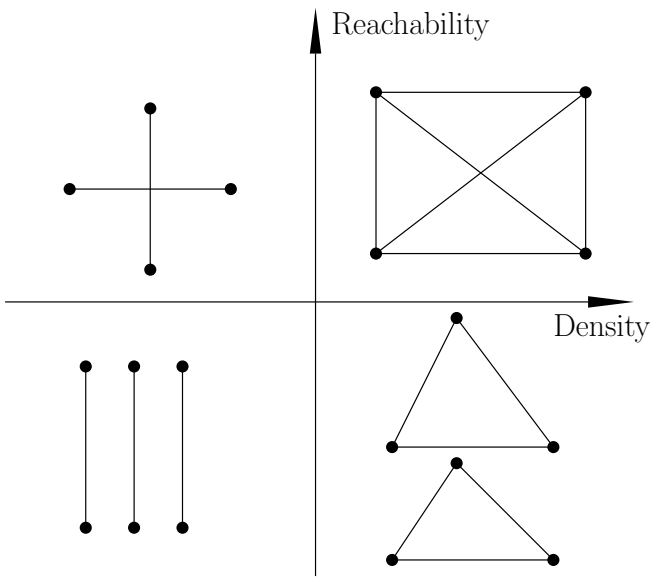

Fig. 1. Different types of networks as a function of reachability and density [4].

Figure. 1 shows the difference of some graphs in terms of density and reachability.

B. Size of the largest connected component

Size of the largest connected component can be determined using different approaches. In our experiments we have calculated the size of the largest singly connected component and the size of the largest biconnected component using a software [5].

C. Topological perturbation of complex networks

Perturbations in complex systems can deactivate some of the edges or nodes. Perturbations are of two types.

- *Edge loss:* The edge is deleted.
- *Node loss:* The node and all its incident edges are deleted.

Effects of node loss and edge loss on the network topology:

- Increase of path lengths.
- Separation into isolated clusters.

More connected network means less effect of an edge removal. Bridges are definite points of vulnerability. The effect of a node removal depends on the number and characteristics of the edges incident on that node. (See Figure 2).

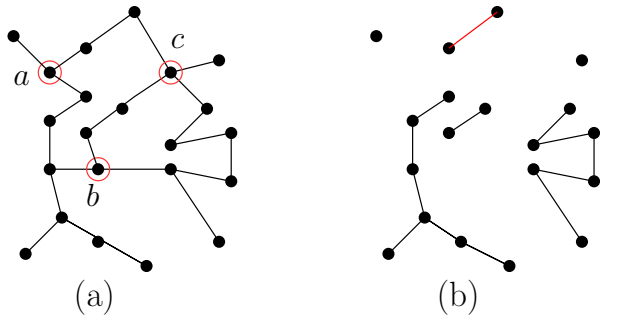

Fig. 2. Effect of node removal; (a) A network and (b) the resulting network after removal of nodes a, b and c.

D. Existing approaches to measure topological robustness

We will give a brief view about the existing formula to find network robustness. The idea of a numeric value of the robustness of a network was first introduced by Piraveenam et al. [3]. They defined a robustness coefficient R of a network of N nodes after removal of k nodes as follows.

$$R = \frac{A_2}{A_1} = \frac{\sum_0^N kS_k}{\frac{N(N+1)(N-1)}{6}} \times 100 \tag{1}$$

Note that A_1 is calculated from an ideal network considering the effect of deleting k nodes one by one as follows.

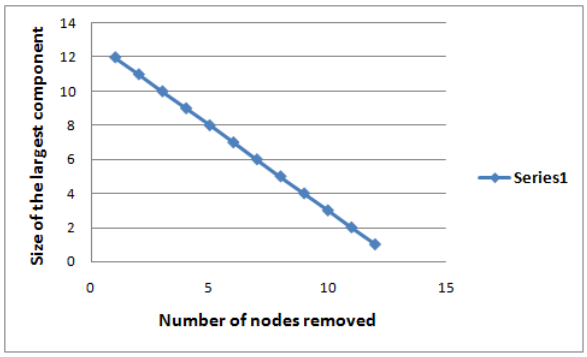

Fig. 3. Size of largest component against the number of nodes removed for an ideal network (targeted attack).

$$\begin{aligned} A_1 &= 0.N + 1.(N-1) + 2.(N-2) + ... + (N-1).1 + N.0 \\ &= \sum_0^N k(N-k) \\ &= \sum_0^N k.N - \sum_0^N k^2 \\ &= N(N/2)(N+1) - (N/6)(N+1)(2N+1) \\ &= (N/6)(N+1)(N-1) \\ &= \frac{N(N+1)(N-1)}{6} \end{aligned} \tag{2}$$

A_2 is calculated considering the size S_k of the largest connected component of an arbitrary network after each deletion as follows.

$$A_2 = \sum_0^N kS_k \tag{3}$$

Obviously higher value of R indicates slow disintegration of the network.

III. Biconnectivity as an approach for network reliability and robustness

From some previous works [1] [2] [3], the existence of a giant connected component i.e. a connected component of size comparable to the system size N, is considered an indicator of structural robustness of the entire system. Slow disintegration of this component cannot always represent robustness of the network in terms of reliability. Our approach is to consider a largest biconnected component of the network during the process of node removal. A biconnected component has more than one node-disjoint path between every pair of nodes. In the presence of external or internal perturbations, two disjoint paths connecting two nodes can communicate and function even under the failure of one pathway. A system with a giant biconnected component can therefore achieve functional stability even when some parts are broken.

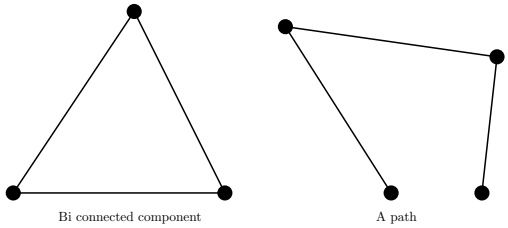

Fig. 4. Components.

Figure. 4 shows two connected components of a graph. There exists only paths or trees in the network, when biconnected components are completely removed. A path is still reachable or connected though density of the network has decreased. We continued to remove node from the network until the network is left with isolated vertices only. Let, S_{sc} be the size of the largest singly connected component and let S_{bc} be the size of the largest biconnected component. In real world complex networks there could be millions of nodes and thousands of connected components. Situation may arise where biconnected component will not be the largest connected component. In fact, if a segment with biconnectivity is actually small in comparison to the total size of the network or to the largest connected component, then robustness will be measured using other metrics. We take a threshold

$$\frac{S_{bc}}{S_{sc}} = 0.1 \tag{4}$$

for considering the contribution of the largest biconnected component and the largest singly connected component in the robustness coefficient. When this ratio will be less than or equal to 0.1, we will consider the other largest connected components for measuring robustness of that network. In our

experiments, three cases are considered when deleting nodes from an arbitrary network.

In case 1, we have considered only the size of the largest singly connected component. In this case, the disintegration may look like Fig. 5.

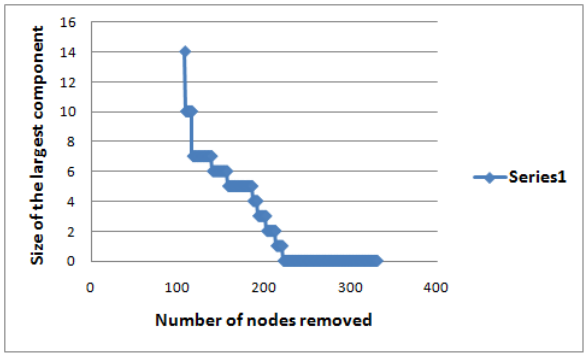

Fig. 5. Disintegration of network, considering the size of the largest singly connected component (targeted attack).

$\sum_0^N kS_{sc}$ represents the area under the profile containing Fig. 5. Here, k represents the number of nodes removed and S_{sc} represents the size of the largest connected component after each removal.

In case 2, we have considered only the size of the largest biconnected component where the area is calculated using $\sum_0^N kS_{bc}$. Here the disintegration looks like Fig. 6.

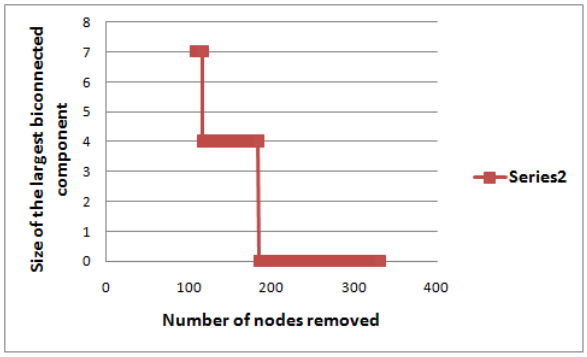

Fig. 6. Disintegration of network, considering the size of the largest biconnected component (targeted attack).

In case 3, we have considered both singly connected and biconnected components. Disintegration looks like Fig. 7. Here, we calculate the area combining both $\sum_0^N kS_{bc}$ and $\sum_0^N kS_{sc} - S_{bc}$.

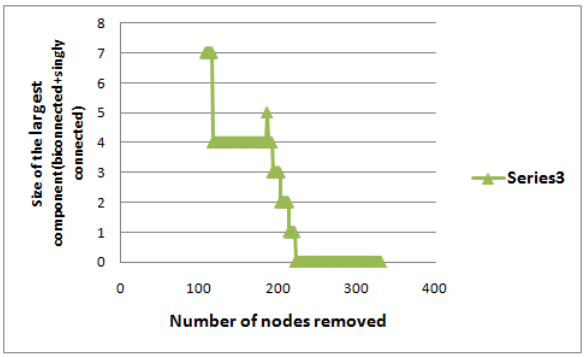

Fig. 7. Disintegration of network, considering the size of the largest biconnected and singly connected component (targeted attack).

$\sum_0^N kS_{bc}$ represents the strictly robust part of the network that contains only the largest biconnected components and $\sum_0^N kS_{sc} - S_{bc}$ represents the rest of the network which contains the largest singly connected component. Combining both we compute A2 as follows.

$$A_2 = \sum_0^N kS_{bc} + \sum_0^N k(S_{sc} - S_{bc}) \tag{5}$$

Using Eqs. (2) and (5) we compute the robustness coefficient R as follows.

$$R = \frac{A_2}{A_1} = \frac{\sum_0^N kS_{bc} + \sum_0^N k(S_{sc} - S_{bc})}{\frac{N(N+1)(N-1)}{6}} \times 100 \tag{6}$$

IV. RESULTS AND DISCUSSIONS

In this section we will demonstrate the results of our experiments. We have applied Eqs. (1) and (6) to several networks to calculate the robustness coefficient of the network. Our first example is a network [6] with 332 vertices. It is a network based on the data of US airline. Fig. 8 represents the disintegration of the network when targeted attack is considered.

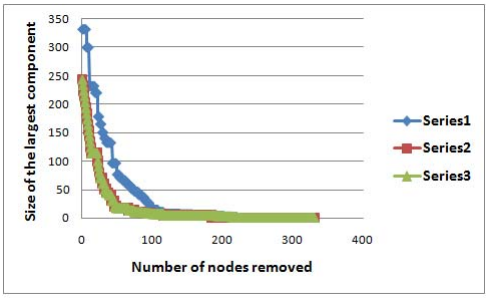

Fig. 8. Disintegration of network (targeted attack).

These curves are functions of number of vertices removed from the largest connected component of the network. Here, x-axis represents the number of vertices removed from the network and y-axis represents the change in size of the largest connected component of the network. This is the case when nodes are removed sequentially from the network. In this figure

Series 1 represents disintegration of the largest connected component of the network. We compute the robustness coefficient using Eq. (1) for Series 1. Though network disintegrates slowly, it can't give clear idea about strict robustness of the network. Series 2 represents disintegration when only size of the largest biconnected component is considered. It demonstrates fragmentation of the strictly robust part of the network. Series 3 represents disintegration when biconnected in addition with other connected components are considered. Robustness coefficient is measured using Eq. (6) for Series 3. At some point of this disintegration process, biconnected components completely disappear and the rest of the largest connected components of the network disintegrate almost linearly. At this point Series 3 overlaps with Series 1 and Series 2 falls to zero. Fig. 9 gives a better view of the disintegration process. It represents the overlap of Series 3 and Series 1. The values of the robustness coefficient R are 94.97, 56.31 and 56.72 for Series 1, Series 2 and Series 3 respectively in the case of targeted attack.

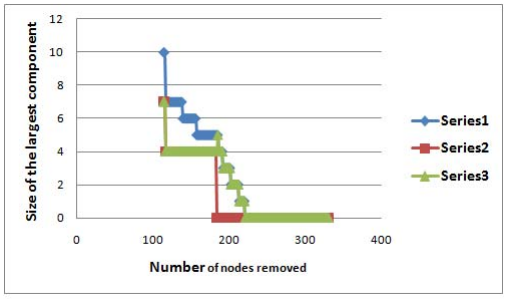

Fig. 9. Disintegration of network (targeted attack).

Figure. 10 represents the disintegration of the network when random attack is considered.

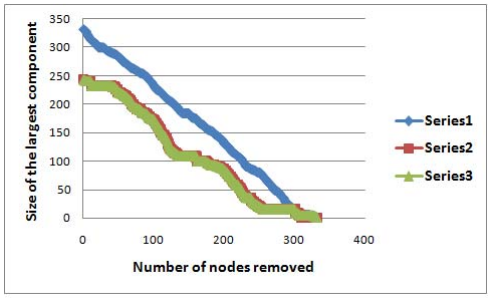

Fig. 10. Disintegration of network (random attack).

Figure. 11 represents the overlap of Series 3 and Series 1 during random attack. Here, the values of the robustness coefficients R are 75.17, 28.73 and 31.76 for Series 1, Series 2 and Series 3 respectively.

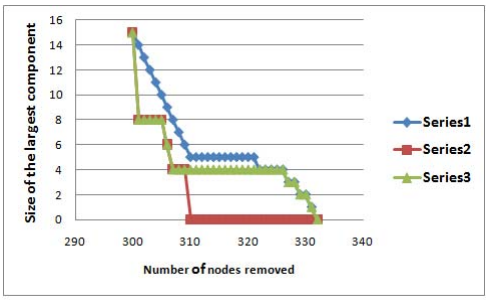

Fig. 11. Disintegration of network (random attack).

We have analyzed another network of 24 vertices. Figure. 12 demonstrates the disintegration of the network. The values of the robustness coefficient R are 58.04, 28.17 and 45.09 for Series 1, Series 2 and Series 3 respectively in the case of targeted attack.

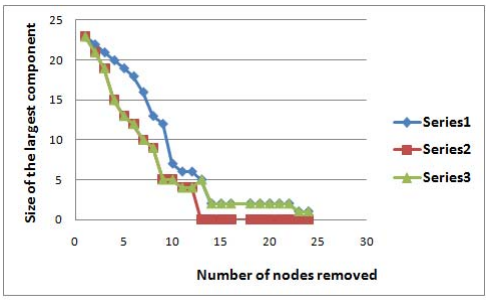

Fig. 12. Disintegration of network (targeted attack).

Our second calculation in Fig. 13 demonstrates the scenario when nodes are removed randomly from the network.

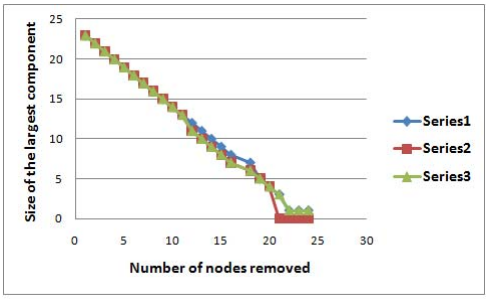

Fig. 13. Disintegration of network (random failure).

Here, the values of the robustness coefficient R are 94.04, 85.49 and 90.10 for Series 1, Series 2 and Series 3 respectively. Analyzing these networks we have found one special case that is, sometimes size of the largest biconnected component is ignorable comparing to size of the largest singly connected component. In that case, we have given priority to size of the largest singly connected component in our calculation of robustness coefficient. We have used Eq. (4) to measure this ratio between size of the largest biconnected component and size of the largest singly connected component. Considering this fact we have analyzed two large networks [7] [8]. One is

of 23,219 vertices and another is of 10,617 vertices. For the first network the robustness coefficient is 66.64 for random attack and 10.36 for targeted attack. For the second network the robustness coefficient is 19.56 for random attack and 6.79 for targeted attack. The value of R during random attack is greater than the value of R during targeted attack. Higher value of R means slow disintegration of the network. From experimental results and discussions it is found that, scale-free networks are more vulnerable to sustained targeted attacks and more resilient to random failures.

V. Conclusion

The reliability of robustness co-efficient depends on the approach used for calculating the co-efficient. The largest connected component size gives a good overall view of the robustness of the whole network. The largest biconnected component size gives an even transparent view of the network robustness. With the sequential deletion of nodes, the resultant largest connected component size decreases too. There are some vertices in that largest component, removal of which breaks that component into several fragments. These vertices works as weak points in that largest connected component. Biconnected components are free from such weak points. Hence if biconnected components are used instead of connected components, we will get a more reliable measurement of robustness of that network. We have adopted largest biconnected component approach and showed that a network shows more resilience when nodes are deleted from the network randomly than targeted manner.

References

[1] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, 2000.

[2] P. Crucittia, M. M. Vito Latora, and A. Rapisarda, "Error and attack tolerance of complex networks," *Physica A*, vol. 340, pp. 388–394, 2004.

[3] M. Piraveenan, S. Uddin, and K. S. K. Chung, "Measuring topological robustness of networks under sustained targeted attacks," in *Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2012)*. IEEE Computer Society, 2012, pp. 38–45.

[4] L. R. Izquierdo and R. A. Hanneman, "Introduction to the formal analysis of social networks using mathematica," *International Journal of Web and Semantic Technology*, vol. 4, no. 2, April 2013.

[5] Pajek, "Program for large network analysis," 2008. [Online]. Available: http://vlado.fmf.uni-lj.si/pub/networks/pajek/

[6] P. Dataset, "Network dataset," 2008. [Online]. Available: http://vlado.fmf.uni-lj.si/pub/networks/

[7] "The edinburgh associative thesaurus dataset," 2014. [Online]. Available: http://vlado.fmf.uni-lj.si/pub/networks/data/dic/eat/Eat.htm

[8] "The university of south florida word association, rhyme, and word fragment norms dataset," 2014. [Online]. Available: http://vlado.fmf.uni-lj.si/pub/networks/data/dic/fa/FreeAssoc.htm

[9] D. B. West, *Introduction to Graph Theory*. New Jersey: Prentice Hall, 2003.

[10] R. Cohen and S. Havlin, *Complex Networks Structure, Robustness and Function*. Cambridge: Cambridge University Press, 2010.

[11] M. Janssen, M. Schoonc, W. Kee, and K. Brnere, "Scholarly networks on resilience, vulnerability and adaptation within the human dimensions of global environmental change," *Science Direct*, vol. 16, no. 3, pp. 240–252, 2006.

[12] M. Duenas, O. Ivanov, X. Lu, and I. Wood, "Robustness in a space of complex networks," *Journal of Physics A: Mathematical and General*, vol. 38, no. 45, pp. 9741– 9749, 2012.

[13] R. Albert and A.-L. Barabási, "Statistical mechanics of complex networks," *Reviews of modern physics*, vol. 74, no. 1, p. 47, 2002.