Network robustness and topological characteristics in scale-free networks

Dharshana Kasthurirathna
Centre for Complex Systems Research
Faculty of Engineering and IT
The University of Sydney
NSW 2006
Australia
Email: dkas2394@uni.sydney.edu.au

Mahendra Piraveenan
Centre for Complex Systems Research
Faculty of Engineering and IT
The University of Sydney
NSW 2006
Australia
Email: mahendrarajah.piraveenan@sydney.edu.au

Gnanakumar Thedchanamoorthy
Centre for Complex Systems Research
Faculty of Engineering and IT
The University of Sydney
NSW 2006
Australia
Email: gthe3845@uni.sydney.edu.au

***Abstract*—In this paper, we explore the relationship between the topological characteristics of a complex network and its robustness to sustained targeted attacks. Using synthesized scale-free networks, we look at a number of network measures, including rich club profiles, scale-free exponent, modularity, assortativity, average path length and clustering coefficient of a network, and how each of these influence the robustness of a scale-free network under targeted attacks. We consider sustained targeted attacks by order of node degree. We show that assortativity and average path length have a positive correlation with network robustness, whereas clustering coefficient has a negative correlation. We did not find any correlation between the modularity and robustness, scale-free exponent and robustness, or rich-club profiles and robustness. Our results highlight the importance of topological characteristics in influencing network robustness, and illustrate design strategies network designers can use to increase the robustness of scale-free networks under sustained targeted attacks.**

I. Introduction

The study of complex networks has been one of the dominant trends in scientific research in the last decade [1], [2], [3], [4], [5], [6], [7], [8]. Scientists from areas as diverse as physics and computer science, mathematics and biology, chemistry and social science have been interested in analysing complex networks in their respective fields and find common features between them. A number of topological metrics have been proposed to understand the structure of a complex network: these include modularity, assortativity, information content, network diameter, and clustering coefficient among others [1], [3], [4], [9]. Meanwhile, researchers have also been interested in the functional features of networks, including their functional motifs, the routing and sharing of information over them, and how they respond to random or targeted attacks.

It has been shown that the ability of a network to maintain its integrity under node failures or attacks depends heavily on its topological structure. For example, scale-free networks are more resilient against random attacks, but more vulnerable to targeted attacks, compared to Erdos-Renyi random networks [10]. It can be immediately seen that quantifying such resilience (robustness) of a network is vital in a number of disciplines. For example, computer networks should be designed in such a way that they should function properly when some nodes (routers or hosts) fail, by technical faults or under attack. On the other hand, in a network of terrorist cells, we might be interested in the best strategy to attack the network so as it is disabled and disintegrated as quickly as possible. Therefore, measuring and comparing the robustness of networks under various failure and attack scenarios is of vital importance.

Since network robustness depends on its topology, there must be quantifiable relationships between topological metrics and the robustness of a network. In this paper, we discuss the relationship of a particular type of robustness measure to a number of topological parameters. The robustness measure is chosen such that it is applicable to sustained targeted attacks which follow a particular algorithm or pattern. In particular, we consider a range of scale-free networks and consider their topological features, analysing how each feature affects its robustness.

The rest of the paper is arranged in the following manner: We will first introduce the network matrices that we will be using to quantify the topological features of a network. Then we will present the robustness metric that we will be using to quantify a scale-free network's robustness under sustained targeted attacks. In the following section, we will present our

978-1-4673-5855-2/13/$31.00 ©2013 IEEE

simulation results and analyse them. In the final section we will present our conclusions.

II. Background

Scale-free networks: Scale-free networks are those networks that display similar topological features irrespective of scale [1], [5]. Such networks are described by power law degree distributions, formally specified as

$$p_k = Ak^{-\gamma}U(k/k_{max}) \tag{1}$$

U is a step function specifying a cut off at $k = k_{max}$. The degree distribution of scale-free networks can be specified by a number of parameters, including maximum degree k_{max}, scale-free exponent γ, proportion of out-lier nodes A, and average degree $\bar{k}$. However, it can be shown that there are only two independent parameters and the others could be derived from these.

Scale-free networks are impressively robust to random node failure and random damage [10], [3]. To destroy or fragment such networks randomly, one would have to remove almost all of its nodes [3]. This perhaps explains, at least partly, why scale-free architecture is commonly found in many evolved networks in nature. This also means that targeted attacks have to be designed specifically to effectively destroy such networks, and non-trivial topological analysis of the network is necessary to identify the nodes to be targeted.

Indeed, most real world networks are scale-free networks, including technical, biological and social networks [11], [12], [13], [14], [3], [15], [5]. It is possible in some directed networks that the in-degree distribution is scale-free but the out-degree distribution is not, or vice versa. For example, the in-degree distributions of some transcription networks are scale-free, while the out-degree distributions are exponential [2]. There are a number of growth models which generate scale-free networks, and prominent among them is the Barabasi-Albert model [1].

Now let us introduce the metrics we will use to analyse the topology of a network.

Assortativity : Assortativity is the tendency observed in networks where nodes mostly connect with similar nodes. Typically, this similarity is interpreted in terms of degrees of nodes. Assortativity has been formally defined as a correlation function of excess degree distributions and link distribution of a network [16], [9]. The concepts of degree distribution $p(k)$ and excess degree distribution $q(k)$ for undirected networks are well known [9]. Given $q(k)$, one can introduce the quantity $e_{j,k}$ as the joint probability distribution of the remaining degrees of the two nodes at either end of a randomly chosen link. Given these distributions, the assortativity of an undirected network is defined as:

$$\rho = \frac{1}{\sigma_q^2}\left[\sum_{jk} jk\left(e_{j,k} - q_j q_k\right)\right] \tag{2}$$

where σ_q is the standard deviation of $q(k)$. Assortativity distributions can be constructed by considering the local assortativity of all nodes in a network [17], [18].

Modularity: Network modularity is the extent to which a network can be separated into independent sub-networks. Formally[2], modularity quantifies the fraction of links that are within the respective modules compared to all links in a network. [2] introduces an algorithm which can partition a network into k modules and measure the partitions modularity Q. The measure uses the concept that a good partition of a network should have a lot of within-module links and a very small number of between-module links. The modularity can be written as:

$$Q = \sum\nolimits_{s=1}^{k}\left[\frac{l_s}{L} - \left(\frac{d_s}{2L}\right)^2\right], \tag{3}$$

where k is the number of modules, L is the number of links in the network, l_s is the number of links between nodes in module s, and d_s is the sum of degrees of nodes in module s. To avoid getting a single module in all cases, this measure imposes $Q = 0$ if all nodes are in the same module or nodes are placed randomly into modules.

Clustering coefficient: The clustering coefficient of a node characterizes the density of links in the environment closest to a node. Formally, the clustering coefficient C of a node is the ratio between the total number y of links connecting its neighbours and the total number of all possible links between all these z nearest neighbours [3]:

$$C = \frac{2y}{z\left(z-1\right)} \tag{4}$$

The clustering coefficient $\overline{C}$ for a network is the average C over all nodes.

Average Path Length: The average path length l of a network is defined as the average length of shortest paths between all pairs of nodes in that network. For many real world networks, this average path length is much smaller than the size of the network, that is $l \ll N$. Such networks are said to be showing the small world property [19], [20], [21].

$$l_G = \frac{1}{n(n-1)}\sum_{i,j} d\left(v_i, v_j\right) \tag{5}$$

Equation 5 gives the formal definition of the average path length of a network. Here $d(v_i, v_j)$ is the shortest path between the nodes v_i and v_j, and n is the size of the network.

Rich club connectivity: A rich-club is defined in terms of degree-based rank r of nodes, and the rich-club connectivity $\varphi(r)$. The degree-based rank denotes the rank of a given node when all nodes are ordered in terms of their degrees, highest first. This is then normalised by the total number of nodes. The rich-club connectivity is defined as the ratio of actual number of links over the maximum possible number of links between nodes with rank less than r. Thus, it is possible to calculate the rich-club connectivity distribution of a network, $\varphi(r)$ over r. Equation 6 shows the formal definition of the rich-club coefficient.

$$\varphi(r) = \frac{2E(r)}{r(r-1)} \tag{6}$$

Here, $E(r)$ is the number of links between the r nodes and $r(r-1)/2$ is the maximum number of links that these nodes have share.

III. Quantifying the Robustness of a network

In this section we will discuss network robustness and how we propose to quantify it. The ability of a network to perform its intended function depends on how it responds to pressures - both internal and external. Such pressures could include errors, random attacks, targeted attacks based on some criteria, and malevolent and sustained attacks which remove nodes in sequence. The ability of a network to withstand such pressures has been variously called error tolerance, attack tolerance, resilience or robustness of a network, depending on the context [10], [22], [23], [24], [25], [26]. In this paper, we are interested in the ability of a network to resist complete topological disintegration in the face of random or targeted node removals. We will call this topological / structural robustness, or simply robustness of a network.

Indeed there is a substantial body of work which introduces and analyses structural robustness measures. Albert et al. [10] considered error and attack tolerance of complex networks in the following manner. They removed nodes from complex networks one by one until all nodes are extracted (we will call this 'sustained attack', as opposed to an attack where only a portion of the nodes are ever removed), and studied the variation of topological properties in networks due to these removals. They removed nodes in two separate orders- (i) Random order (ii) Ordered by degree (highest degree first). They analyzed the following three topological properties:

1) Network diameter
2) The size of the largest component
3) The average size of the rest of the components

Albert et al. [10] however relied on profiles of quantities, rather than a single robustness measure, to demonstrate these facts. Following their work, a plethora of metrics have been proposed to measure the topological robustness of networks as a single quantity. However, they typically calculate averaged effects of single node removals, rather than effects of sequential removals, or are too simplistic. For example, the *network efficiency* has been defined as the average of inverted shortest path lengths [23], and used for quantifying the robustness of a network. Node removals are not explicitly considered in this measure.

Similarly, Dekker and Colbert [24] introduced two concepts of connectivity for a graph which can be used to model network robustness: the *node connectivity* and *link connectivity*, which are the smallest number of nodes and links respectively, whose removal results in a disconnected or single-node graph.

In this paper, we choose to use a particular robustness measure which helps us quantify a network's resilience under sustained targeted attacks. It has the advantage of providing a single numeric value to quantify the topological robustness of a network under sustained attack. We use the robustness coefficient introduced in a recent work [27],[28], which is applicable to persistent targeted attacks. The coefficient is based on the size of the largest component S_k of the network after k timesteps, and how it changes over those k timesteps as nodes are serially removed. If we consider the size of the largest component of a network which is under persistent attack, the largest component size S_k vs the number of nodes removed (or number of time steps) k profile may look like Fig. 1 for a small network.

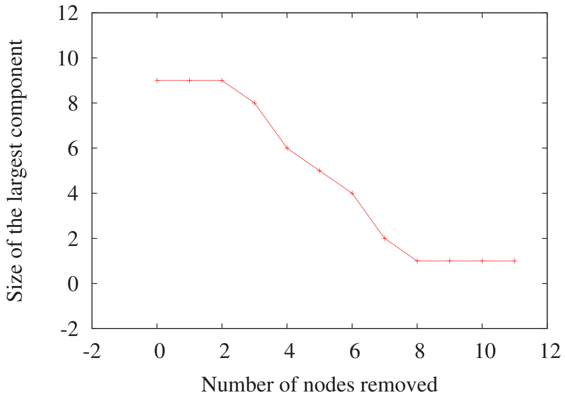


Fig. 1: Size of largest component against the number of nodes removed for a network under sustained targeted attack

Now let us consider an 'ideal' network in terms of robustness under sustained attack. If the network resists disintegration, the S_k of such network should decrease by unity each time a node is removed. That is, the size of largest component decreases only by the removed node, while all other nodes remain part of the largest (single) component until they are themselves removed. S_k will become unity only when all nodes except one have been removed / destroyed. The S_k vs nodes removed profile of such an ideal network with $N = 11$ may look like Fig. 2:

Robustness coefficient [27],[28] proposes that the ratio of areas under two such profiles define the topological robustness under sustained attack for any network. The reasoning behind this formulation is that, for an ideally robust network the size of the largest component will decrease linearly, while the more non-robust the network is, the quicker it will collapse, and the change in the size of the largest component will reflect this collapse.

The area under first profile could be calculated as:

$$A_1 = 0.5S_0 + \sum_{k=1}^{N-1} S_k + 0.5S_N \tag{7}$$

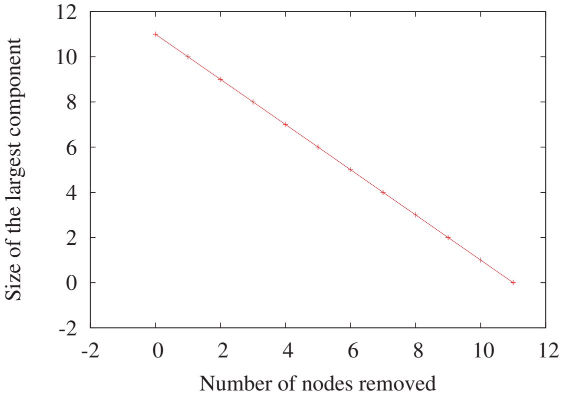


Fig. 2: Size of largest component against the number of nodes removed for an ideally robust network under targeted attack

Here S_0 is the initial largest component size. Since S_N, the size of the largest component after N nodes are removed, is by definition zero, we may say that

$$A_1 = \sum_{k=0}^{N} S_k - 0.5S_0 \tag{8}$$

Meanwhile, the area under the second profile would be given by

$$A_2 = (1/2)N^2 \tag{9}$$

Because after each node removal, a size of the largest component will reduce only by a single node.

Therefore the robustness coefficient measure [27],[28] is given by:

$$R = \frac{A_1}{A_2} = \frac{2\sum_{k=0}^{N} S_k - S_0}{N^2} \tag{10}$$

Since R is always less than unity and often is a very small (non-negative) quantity, it is suitable to define it as a percentage. That is:

$$R = \frac{A_1}{A_2} = \frac{200\sum_{k=0}^{N} S_k - 100S_0}{N^2} \tag{11}$$

It can be verified that the above definition gives $R = 100\%$ for a fully connected network of any size, as expected.

It can be easily seen that the quicker a network begins to disintegrate, the smaller this coefficient will be. However, it also captures the largest component profile before and after the phase transition point by considering the area under this profile. Therefore this measure is superior to the phase-transition time T_{pt} which only indicates the time-steps (or number of nodes) needed before a network begins to disintegrate.

IV. Simulation results

We used a total of 100 synthesized scale-free networks in our simulation. The networks were synthesized using a variant of the Preferential Attachment (PA) method, widely used as a model to synthesize scale-free networks [1]. Each network consisted of 1000 nodes. The network size was chosen arbitrarily, while considering the computing time that would be necessary to compute the properties of a much larger network. We chose four different link-to-node ratio (LNR) values, namely $LNR = 2, 3, 4$ and 5. We had twenty-five networks with each LNR value, and these networks were different from each other in topological characteristics such as scale-free exponent, modularity, clustering coefficient, assortativity, rich-club profile, and average path length.

When attacking the networks, we used a degree based attack. In other words, we removed the node with the highest degree form the network, in each iteration. When there are multiple nodes with the highest degree, a randomly selected node out of those is removed. In doing so, we assume that the degrees of all nodes are known prior to the attack. All the robustness results obtained are dependent on the type of attack used. If a different type of attack was used, that would have affected the resulting robustness values.

We measured the robustness of each of these networks using the robustness metric described above. The topological robustness is measured as a percentage and illustrates the network's ability to withstand sustained targeted node removal. We removed the nodes in the order of node degree[1].

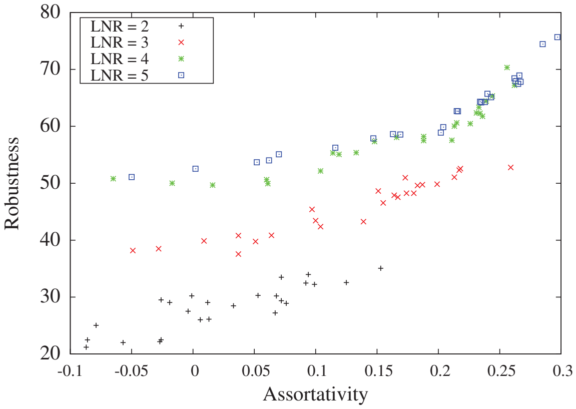


Fig. 3: Network robustness against network assortativity. Four different link-to-node ratios ($LNR = 2, LNR = 3, LNR = 4, LNR = 5$) are considered.

We now analyse how the network robustness depends on each of the topological characteristics mentioned above. Our

[1] Due to space restrictions in this exploratory paper, we avoid showing our results in tables, and show results through figures only.

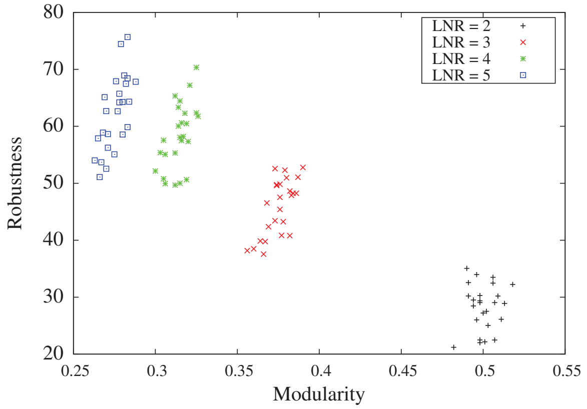


Fig. 4: Network robustness against network modularity. Four different link-to-node ratios ($LNR = 2, LNR = 3, LNR = 4, LNR = 5$) are considered.

results are illustrated in figures 3-8. In Fig. 3, we plot the network robustness against network assortativity. The figure shows that robustness tends to increase with assortativity. This could be explained by the fact that, high assortativity means similar nodes (in terms of degrees) are connected together, including the hubs. Therefore, compared to a non-assortative scale-free network, the hubs in assortative scale-free networks have 'back-ups', hence making it harder for the network to be broken apart by targeted attacks. Fig. 4 shows robustness against network modularity. We find that modularity has no correlation with network robustness. Fig. 5 shows robustness against clustering coefficient. It can be seen that from Fig. 5 that these quantities are negatively correlated, with higher clustering coefficient resulting in low robustness. While this may seem counter-intuitive, it could be explained by the fact that the more clustering a network has, the less proportion of the links will be between distant parts of the network (this also explains the negative correlation usually observed between clustering coefficient and average path length), and as such, the network could be broken apart into components easily. While these components themselves will be quite robust to further attacks, the early disintegration means the robustness coefficient will be small for networks with high clustering.

Fig. 6 shows network robustness against average path length. As expected (and explained above) there is positive correlation between average path length and network robustness. In Fig. 7 we show network robustness against scale-free exponents. We see that the correlation pattern varies here. While it is well known that scale-free networks are more vulnerable to targeted attacks compared to random networks [10], let us point out that the scale-free exponent is *not* a measure of the *scale-freeness* of a network. Therefore, the networks with high scale-free exponents are not necessarily more scale-free than those with lower scale-free exponents. Indeed, we found that in the networks we simulated, there was a correlation between the squared error of fitting a scale-free exponent to a network, and the exponent itself, which means

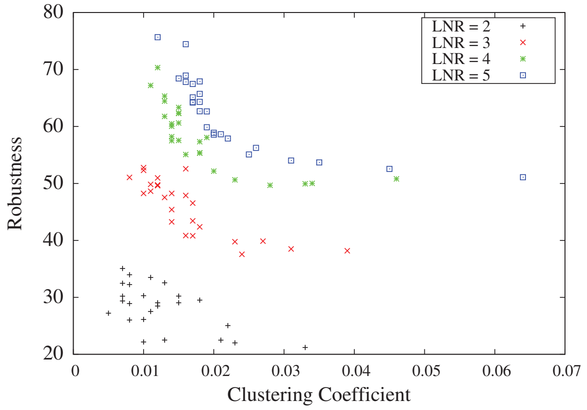


Fig. 5: Network robustness against network clustering coefficient. Four different link-to-node ratios ($LNR = 2, LNR = 3, LNR = 4, LNR = 5$) are considered.

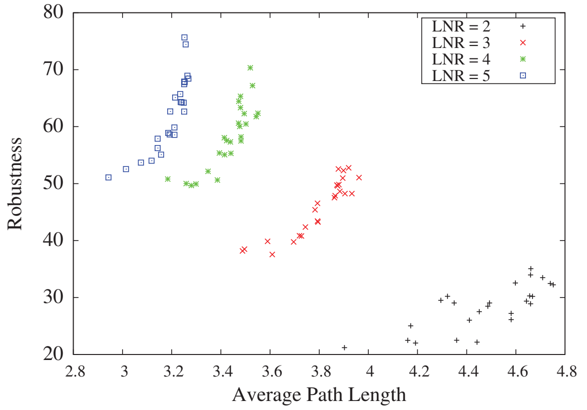


Fig. 6: Network robustness against network average path length. Four different link-to-node ratios ($LNR = 2, LNR = 3, LNR = 4, LNR = 5$) are considered.

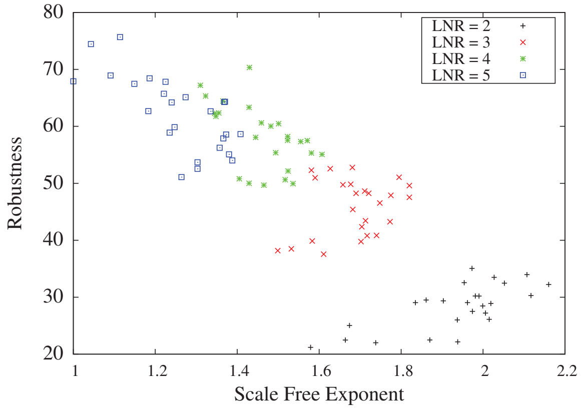


Fig. 7: Network robustness against network scale-free exponent. Four different link-to-node ratios ($LNR = 2, LNR = 3, LNR = 4, LNR = 5$) are considered.

that the higher the scale-free exponent, the less the scale-free characteristic of a network (though the error in all cases was small enough to justify the network being identified as scale-free).

We also considered the rich-club profiles of each of the networks we studied. Since the rich-club profile is not a single quantity, we considered the rich-club coefficient of the network at four percentile values, namely 5%, 10%, 15%, and 20% (for example, a 5% rich-club coefficient meant that the sub-network consisting of the top 5% nodes (in terms of degrees) was considered to calculate the rich club.). However, as Fig. 8 shows, the rich-club phenomena does not seem to affect the robustness of networks. It may be the case that smaller rich-clubs have an effect on network robustness, and a more detailed study exploring the whole rich-club profile of each network is necessary to determine the exact effect of rich-clubs on network robustness. Such a study is beyond the scope of this exploratory paper.

V. Discussion

In order to quantitatively observe the relationships between the different network properties and the robustness coefficient values, we calculated the Pearson correlation coefficient values between them. Table I summarises the results of those calculations. These calculations were done for the networks with four different link-to-node ratios (LNR).

TABLE I: Pearson correlation coefficients between the different network properties considered and the robustness coefficient values. Networks with four different link-to-node ratios (LNR) were considered.

	LNR = 2.0	**3.0**	**4.0**	**5.0**
Assortativity	0.86	0.95	0.9	0.92
Modularity	0.09	0.7	0.58	0.7
Clustering Coefficient	-0.59	-0.8	-0.76	-0.75
Average Path Length	0.76	0.9	0.84	0.83
Scale-free Exponent (γ)	0.71	0.28	-0.55	-0.7
Rich Club Coefficient				
5%	0.32	-0.18	0.35	0.18
10%	0.4	-0.11	0.27	-0.25
15%	-0.39	-0.309	-0.14	0.07
20%	-0.43	-0.24	0.04	0.11

Let us now discuss a few implications and limitations of our results. According to the above results, assortativity and the robustness coefficient show a clear positive correlation. Assortativity is a measure of the similarity of the nodes that are connected, in terms of the node degree [29]. Hence, this result implies that when there are more connections among similar nodes, we can expect to see a higher topological robustness in that particular network. However, let us note that most networks we considered have positive assortativity. Those networks which were disassortative were only marginally so. Therefore, it is difficult to say whether the absolute value of assortativity has a positive correlation with network robustness.

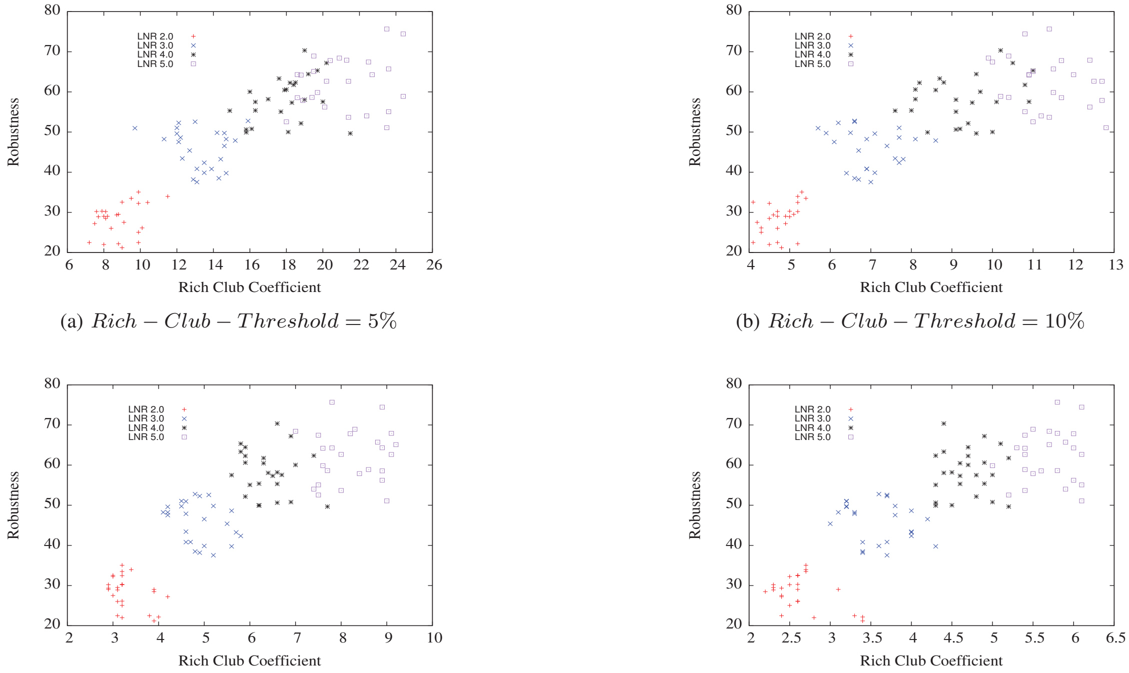
The next point to note is that modularity does not seem to substantially influence network robustness. This is welcome from a network designer's point of view, since modular networks could be designed without compromising the robustness of a network. Many evolved and synthesized networks in social and engineered systems are modular[2]. Furthermore, in some systems such as software networks, there is a need to design the network as a modular network [27],[28]. Therefore it is significant that modular networks could be designed without compromising the attack tolerance of a network.

As mentioned above, clustering coefficient tends to have a negative correlation with average path length, when an ensemble of networks is considered [30]. Networks with relatively small average path length and high clustering correlation are called small world networks [1], [31]. Our results show that the smaller the clustering coefficient is, and the larger the average path length is, the higher the robustness. This must mean that small world networks are relatively not robust to sustained targeted attacks. Just like scale-free networks which are not robust to targeted attacks compared to random networks [10], [23], many natural networks which are small-world networks also achieve their 'small-worldness' at the cost of robustness to sustained targeted attacks.

It is already known that scale-free networks are more resilient to random node failures, compared to random networks. That is, preferential mixing is likely to increase network robustness. Preferential mixing indicates that the nodes that have higher degrees have a higher probability of attracting new links. Examples of such networks include scientific collaboration networks and social networks. Such networks generally demonstrate scale-free degree distributions [1]. Note well that random mixing does not necessarily imply the topology itself is random (such as an Erdos-Renyi network). Indeed, many scale-free networks, both synthesized and real world, can show near random mixing patterns [16], [17], [18], [9].

With that background in mind, we may evaluate the correlation results between the scale-free exponent γ and the robustness coefficient. When the link-to-node ratio increases, there's a deviation of the scale-free exponent from its commonly observed window of 2 to 3 [1]. Moreover, the correlation between the scale-free exponent and robustness coefficient transform from positive to negative, as the link-to-node ratio increases. This may suggest that the scale-free nature of a network could have an effect on the topological robustness of a network. However, we failed to observe a strong correlation between the scale-free exponent and the robustness coefficient. This could be partly due to the fact that we used a degree based attack to disintegrate the network, instead of emulating random node failures.

Finally, we found that in our analysis there was no correlation between rich-club tendencies and network robustness. However, we need further analysis to come to definitive conclusions here, since the rich-club phenomena cannot be measured by a single number, and is measured through a profile. Networks may show rich club phenomena at various percentile cut-offs, and we did not find that much variation among networks on the cut-offs we chose (5%, 10%, 15%, 20%). Therefore, further analysis may be necessary to



(a) $Rich-Club-Threshold = 5\%$

(b) $Rich-Club-Threshold = 10\%$

(c) $Rich-Club-Threshold = 15\%$

(d) $Rich-Club-Threshold = 20\%$

Fig. 8: Network robustness against network rich-club coefficients. Four different link-to-node ratios ($LNR = 2, LNR = 3, LNR = 4, LNR = 5$) are considered.

establish the influence of rich-club phenomena on network robustness to targeted attacks.

VI. Summary

In this paper, we analysed the relationship of network robustness (under sustained targeted attacks) with a number of topological features in scale-free networks. Using synthesized scale-free networks, we considered topological characteristics including scale-free exponent, modularity, clustering coefficient, assortativity, rich-club profile, and average path length. We used a particular robustness measure designed to analyse resilience under sustained targeted attacks to measure robustness. We designed our attacks based on the order of node degrees.

We found considerable positive correlations between network robustness and the following topological measures: assortativity, average path length and We provided intuitive explanations for why these measures may have a positive correlation with network robustness. We found that the clustering coefficient has a negative correlation with network robustness. We did not find that network modularity, rich-club profile or scale-free exponents affect the robustness of a network one-way or another. We discussed the implications and limitations of our results.

References

[1] R. Albert and A.-L. Barabási, "Statistical mechanics of complex networks," *Reviews of Modern Physics*, vol. 74, pp. 47–97, 2002.

[2] U. Alon, *Introduction to Systems Biology: Design Principles of Biological Circuits*. London: Chapman and Hall, 2007.

[3] S. N. Dorogovtsev and J. F. F. Mendes, *Evolution of Networks: From Biological Nets to the Internet and WWW*. Oxford: Oxford University Press, January 2003.

[4] F. Kepes (Ed), *Biological Networks*. Singapore: World Scientific, 2007.

[5] J. Park and M. E. J. Newman, "Statistical mechanics of networks," *Physical Review E*, vol. 70, no. 6, pp. 066 117+, Dec 2004. [Online]. Available: http://dx.doi.org/10.1103/PhysRevE.70.066117

[6] M. Piraveenan, M. Prokopenko, and A. Y. Zomaya, "Assortative mixing in directed biological networks," *IEEE/ACM Transactions on computational biology and bioinformatics*, vol. 9(1), pp. 66–78, 2012.

[7] M. Piraveenan, M. Prokopenko, and L. Hossain, "Percolation centrality: Quantifying graph-theoretic impact of nodes during percolation in networks," *PloS one*, vol. 8, no. 1, p. e53095, 2013.

[8] M. Piraveenan, M. Prokopenko, and A. Zomaya, "On congruity of nodes and assortative information content in complex networks," *Networks and Heterogeneous Media (NHM)*, vol. 3, no. 10.3934/nhm.2012.7.441, pp. 441–461, 2012.

[9] R. V. Solé and S. Valverde, "Information theory of complex networks: on evolution and architectural constraints," in *Complex Networks*, ser. Lecture Notes in Physics, E. Ben-Naim, H. Frauenfelder, and Z. Toroczkai, Eds. Springer, 2004, vol. 650.

[10] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, pp. 378–382, 2000.

[11] A.-L. Barabási, "Scale-free networks: A decade and beyond," *Science*, vol. 325, no. 5939, pp. 412–413, 2009.

[12] A.-L. Barabási, R. Albert, and H. Jeong, "Scale-free characteristics of random networks: The topology of the world-wide web," *Physica A*, vol. 281, pp. 69–77, 2000.

[13] A.-L. Barabási and E. Bonabeau, "Scale-free networks," *Scientific American*, vol. 288, pp. 50–59, 2003.

[14] A. Cavagna, A. Cimarelli, I. Giardina, G. Parisi, R. Santagati, F. Stefanini, and M. Viale, "Scale-free correlations in bird flocks," 2009, arXiv:0911.4393. [Online]. Available: http://arxiv.org/abs/0911.4393

[15] M. Mitchell, "Complex systems: Network thinking," *Artificial Intelligence*, vol. 170, no. 18, pp. 1194–1212, 2006.

[16] M. E. J. Newman, "Mixing patterns in networks," *Physical Review E*, vol. 67, no. 2, p. 026126, 2003.

[17] M. Piraveenan, M. Prokopenko, and A. Y. Zomaya, "Local assorta-

tiveness in scale-free networks," *Europhysics Letters*, vol. 84, no. 2, p. 28002, 2008.

[18] ——, "Local assortativeness in scale-free networks — addendum," *Europhysics Letters*, vol. 89, no. 4, p. 49901, 2010.

[19] V. Latora and M. Marchiori, "Efficient behavior of small-world networks," *Physical Review Letters*, vol. 87, no. 19, p. 198701, 2001.

[20] M. E. J. Newman, "Models of the small world," *Journal of Statistical Physics*, vol. 101, no. 3, pp. 819–841, November 2000. [Online]. Available: http://dx.doi.org/10.1023/A:1026485807148

[21] D. J. Watts and S. H. Strogatz, "Collective dynamics of small-world networks," *Nature*, vol. 393, no. 6684, pp. 440–442, June 1998. [Online]. Available: http://dx.doi.org/10.1038/30918

[22] L. d. F. Costa, F. A. Rodrigues, G. Travieso, and P. R. Villas Boas, "Characterization of complex networks: A survey of measurements," *Advances in Physics*, vol. 56, no. 1, pp. 167–242, 2007.

[23] P. Crucittia, V. Latora, M. Marchiori, and A. Rapisarda, "Error and attack tolerance of complex networks," *Physica A*, vol. 340, p. 388394, 2004.

[24] A. H. Dekker and B. D. Colbert, "Network robustness and graph topology," in *Proceedings of the 27th Australasian conference on Computer science - Volume 26*, ser. ACSC '04. Darlinghurst, Australia, Australia: Australian Computer Society, Inc., 2004, pp. 359–368.

[25] A. K. S. Ng and J. Efstathiou, "Structural robustness of complex networks," *Physical Review E*, vol. 3, no. 2, pp. 175–188, 2006.

[26] V. Venkatasubramanian, S. Katare, P. R. Patkar, and F. Mu, "Spontaneous emergence of complex optimal networks through evolutionary adaptation," *CoRR*, vol. nlin.AO/0402046, 2004.

[27] M. Piraveenan, G. Thedchanamoorthy, S. Uddin, and K. S. K. Chun, "Quantifying topological robustness of networks under sustained targeted attacks," *Social Network Analysis and Mining*, Under Review.

[28] M. Piraveenan, S. Uddin, and K. S. K. Chung, "Measuring topological robustness of networks under sustained targeted attacks," in *2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*. New York: IEEE Computer Society, 2012.

[29] M. E. J. Newman, "Assortative mixing in networks," *Physical Review Letters*, vol. 89, no. 20, p. 208701, 2002.

[30] J. T. Lizier, M. Piraveenan, D. Pradhana, M. Prokopenko, and L. S. Yaeger, "Functional and structural topologies in evolved neural networks," in *Advances in Artificial Life: Tenth European Conference on Artificial Life (ECAL '09)*, ser. LNCS/LNAI. Springer, 2009, vol. 5777-5778.

[31] S. Milgram, "The small world problem," *Psychology Today*, vol. 1, p. 61, 1967.