Robustness of complex networks to node and cluster damage

Emil Gegov[1], Mark Atherton[1], Hamed Al-Raweshidy[2]

1. Mechanical Engineering, School of Engineering and Design, Brunel University, Uxbridge, Middlesex, UK

2. Electronic & Computer Engineering, School of Engineering and Design, Brunel University, Uxbridge, Middlesex, UK

emil.gegov@brunel.ac.uk

Abstract: The goal of this investigation is to assess the robustness of two popular network structures – random networks and scale-free networks – to node and cluster damage. There is no previous work on the latter. For node damage, we remove nodes iteratively and for cluster damage, we first build a network of clusters and then remove the nodes (clusters).

Keywords: *random network, scale-free network, node damage, cluster damage, error tolerance, attack tolerance*

Introduction

One of the main characteristics of complex networks is their ability to sustain a significant amount of damage, while their functionality virtually remains unaffected [1]. For example, communication networks often experience local failures of core components, but this has no effect on the performance of the rest of the network. The same holds for a vast range of biological networks [2]. Simple organisms often develop, survive and reproduce in the presence of extreme environmental changes, internal failures, or even pharmaceutical interference. This is due to the robustness of the underlying metabolic network.

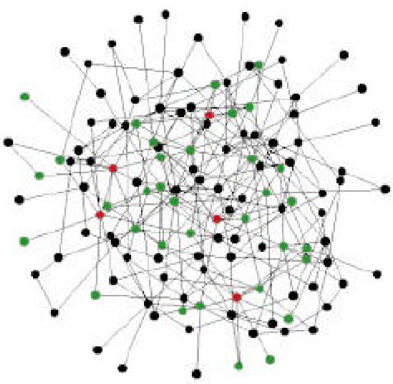

Figure 1. Random network

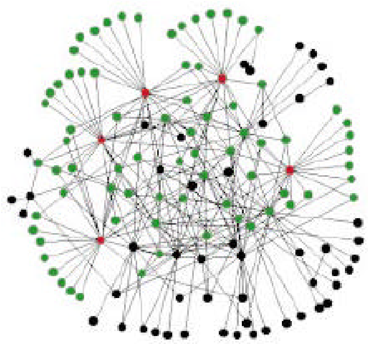

Figure 2. Scale-free network

There are three principle mechanisms of network robustness: redundant components, distributed functionality, and self-organization [3]. Redundancy ensures that if a component fails, there is another identical or similar component, which can carry out the function of the former. However, having back-up components is wasteful and costly, so an alternative is to have multiple heterogeneous components with overlapping (distributed) functions. The most complex mechanism, self-organization, involves concepts, such as modularity, decoupling, feedback control and self-adaptation [4].

Methodology

We investigate two types of network robustness: error and attack tolerance. For the former, components are removed at random. For the latter, components with the highest *betweenness centrality* are removed first, i.e. those, which have the highest proportion of shortest paths going through them. The level of tolerance is measured by two parameters: the average of all shortest paths, and the number of isolated nodes.

For node damage, we proceed by removing nodes iteratively and measuring the two parameters. For cluster damage, the network first needs to be divided into a set of optimum clusters with maximum modularity, as described in [5]. We then represent each cluster by a single node, and cross-cluster links by normal links, in a new *network of clusters*. Finally, we proceed by deleting nodes iteratively to simulate cluster damage.

Discussion

Before damaging the network, it is sensible to calculate the component *betweenness centrality* distribution for two reasons. First, this attribute can be used to predict the sort of results we can expect. Second, the experiment should be justified and supported by this distribution, as it highlights the difference between networks and the distinction between errors and attacks. Similarly, the node degree distribution is the key factor, determining network robustness to attacking high degree nodes.

Conclusion

There will be two main contributions to scientific knowledge to follow from this investigation: to shed some light on the effects of cluster damage in complex networks; and to explore the relationship between node and cluster damage.

References

1. Albert, R., Jeong, H. & Barabasi, A-L. Error and attack tolerance of complex networks. *Nature* **406**, 378-381 (2000).
2. Jeong H. *et al.* The large-scale organisation of metabolic networks. *Nature* **407**, 651-654 (2000).
3. Kitano, H. Biological robustness. *Nature Reviews Genetics* **5** (11), 826-837 (2004).
4. Prehofer, C. & Bettstetter, C. Self-Organization in Communication Networks: Principles and Design Paradigms. *IEEE Communications Magazine* **43** (7), 78-85 (2005).
5. Newman, M. E. J. & Girvan, M. Finding and evaluating community structure in networks. *Physical Review E* **69**, 026113-1-026113-15 (2004).

Figure Legends

1. Illustration of a random network: nodes have roughly the same degree. Red: the five highest degree nodes; Green: their first neighbours. From [1].
2. Illustration of a scale-free network: most nodes have one or two links but a few nodes have a very large number of links. From [1].