Research Letter

Evolving Networks with Enhanced Stability Properties

David Newth¹ and Jeff Ash²

¹ CSIRO Centre for Complex Systems Science, CSIRO Marine and Atmospheric Research, CSIRO, Canberra, ACT, 2601, Australia

² Centre for Research into Complex Systems (CRiCS), Charles Sturt University, Albury, NSW, 2640, Australia

Correspondence should be addressed to David Newth, david.newth@csiro.au

Received 22 April 2008; Accepted 1 October 2008

Recommended by Shlomo Havlin

We use a search algorithm to identify networks with enhanced linear stability properties in this account. We then analyze these networks for topological regularities that explain the source of their stability/instability. Analysis of the structure of networks with enhanced stability properties reveals that these networks are characterized by a highly skewed degree distribution, very short path-length between nodes, little or no clustering, and disassortativity. By contrast, networks with enhanced instability properties have a peaked degree distribution with a small variance, long path-lengths between nodes, a high degree of clustering, and high assortativity. We then test the topological stability of these networks and discover that networks with enhanced stability properties are highly robust to the random removal of nodes, but highly fragile to targeted attacks, while networks with enhanced instability properties are robust to targeted attacks. These network features have implications for the physical and biological networks that surround us.

Copyright © 2008 D. Newth and J. Ash. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1. INTRODUCTION

Our modern society has come to depend on large-scale infrastructure networks to deliver resources to our homes and businesses in an efficient manner. Critical infrastructure is continually confronted with small perturbations, most of which have no effect on the network's performance. However, a small fraction of these disturbances propagates through the network, crippling its performance. Over the past decade, there have been numerous examples where a local disturbance has led to the global failure of critical infrastructure. For instance, on August 14, 2003, a string of events starting in Ohio triggered the largest blackout in North American history [1]. Where a network is carrying a flow of some types (electricity, gas, data packets, information, etc.), a "node" carries a load, and under normal circumstances this load does not exceed the capacity of that node. Nodes also have the ability to mediate the behavior of the network in response to a perturbation (such as the failure of a neighboring node or a sudden local increase in flow). The resilience of a system to the propagation of disturbances is directly related to the structure of the underlying network. In previous work [2] we have examined the topological properties of networks that make them resilient to cascading

failures. In this account, we use a search algorithm to help us identify network properties that lead to enhanced linear stability properties. We also show that networks that display enhanced linear stability properties are highly resilient to the random loss of nodes. By contrast networks with enhanced instability properties tend to be more resilient to the loss of key nodes.

2. STABILITY ANALYSIS OF COMPLEX NETWORKS

Many of the complex systems that surround us—from food webs to critical infrastructure—are large, complex, and grossly nonlinear in their dynamics. Typically, models of these systems are inspired by equations similar to

$$\frac{dX_i}{dt} = F_i(X_1(t), X_2(t), \dots, X_n(t)), \quad (1)$$

where F_i is an empirically inspired, nonlinear function of the effect of the i th system element on the dynamics of the other n elements. When modeling ecological systems, for instance, the function F_i takes on the form of the Lotka-Volterra equations [3]. Of particular interest is the steady state of the system, in which all growth rates are zero, giving

FIGURE 1: Comparison of networks with enhanced stability properties (a), and enhanced instability properties (b).

the fixed point or steady-state values for each of the state variables X_i^* . This occurs when

$$0 = F_i(X_1^*(t), X_2^*(t), \dots, X_n^*(t)). \quad (2)$$

The local dynamics and stability in the neighborhood of the fixed point can be determined by expanding (1) in a Taylor series about the steady state:

$$\begin{aligned} \frac{dX_i(t)}{dt} = & F_i|_* + \sum_{j=1}^n \left[\frac{\partial F_i}{\partial X_j} \right]_* x_j(t) \\ & + \frac{1}{2} \sum_{k=1}^n \left[\frac{\partial^2 F_i}{\partial X_j \partial X_k} \right]_* x_j(t)x_k(t) + \dots, \end{aligned} \quad (3)$$

where $x_i(t) = X_i(t) - X_i^*$ and $*$ denotes the steady state. Since $F_i|_* = 0$, and close to the steady state, the x_i values are small, all terms that are second order and higher need not be considered in determining the stability of the system. This gives a linearized approximation that can be expressed in matrix form as

$$\frac{d\mathbf{x}(t)}{dt} = \mathbf{A}\mathbf{x}(t), \quad (4)$$

where $\mathbf{x}(t)$ is an $n \times 1$ column vector of the deviations from the steady state. As May [4] demonstrates, determining the eigenvalues for $\mathbf{A}$ reveals the stability properties of the system. Specifically the real parts of the eigenvalues can be ordered $|\lambda_1| < |\lambda_2| < \dots < |\lambda_{n-1}| < |\lambda_{\max}|$, and we will refer to $\lambda_{\max}$ as the dominant eigenvalue. If $\lambda_{\max} < 0$, then the system is said to be stable to perturbations in the region of the fixed point. In this account, we use a rewiring scheme to create networks with enhanced stability properties (i.e., $\min[\lambda_{\max}]$), and networks that have enhanced instability properties (i.e., $\max[\lambda_{\max}]$).

3. EVOLVING NETWORKS

We make use of a stochastic rewiring scheme to create networks with the desired stability properties. This rewiring scheme is similar to those used in previous studies [2, 5], and the effectiveness of this algorithm at finding networks with enhanced stability properties is given in [5]. The rewiring

FIGURE 2: Comparison between the evolved networks with enhanced stability properties and the two random null models: (a) average shortest path length; (b) diameter; (c) clustering coefficient; and (d) assortativeness.

scheme consists of three steps: (1) an edge is selected and one end of the edge is reassigned to another node; (2) the dominant eigenvalue ($\lambda'_{\max}$) is calculated for the modified network; and (3) if $\lambda'_{\max}$ is superior to $\lambda_{\max}$, then the edge rewiring is accepted, else it is rejected. These three steps are repeated for 10^5 time steps. The rewiring scheme is initially seeded with an Erdős-Rényi random graph [6] consisting of 100 nodes and 150 edges. The edges are set to a value of 1, but this can be easily modified to take on real values, and the on-diagonal or self-regulating terms are set to -1 . At every step, the network is checked to ensure it consists of a single-connected component. Figure 1 provides two example networks resulting from the maximization and minimization of $\lambda_{\max}$. The structure of the network is then examined for common statistical properties including scale-free degree distribution [7], short path-length and high clustering [8], and assortativeness [9].

4. STRUCTURAL PROPERTIES OF STABLE AND UNSTABLE NETWORKS

For each experiment, 200 runs were made and the final networks collated and analyzed. To determine how “unique” these evolved networks are, we compare their structural characteristics to those of two random null models. The first is an Erdős-Rényi random graph, and is used to determine which characteristics can be accounted for by random structures. The second null model is the degree randomization model as described in [10]. This model randomizes node connection (i.e., which node is connected

FIGURE 3: Comparison between the evolved networks with enhanced instability properties and the two random null models. (a) Average shortest path-length; (b) diameter; (c) clustering coefficient; and (d) assortativeness.

to which other node), but preserves the individual node degree characteristics. Comparison between the evolved networks and the two null models shows those properties that are unique to the evolved networks and can be accounted for by random occurrences, and those that are a consequence of the degree distribution.

Figure 2 shows the comparison between the evolved networks with enhanced stability properties and the two null models. In all cases, the comparisons are drawn from statistics taken from 1000 null models. Figures 2(a) and 2(b) show the variation in the average shortest path-length and diameter. In both cases these characteristics are not significantly different from the degree randomized model. This indicates that these characteristics are directly related to degree distribution. Figure 2(c) compares the clustering between the three models. The evolved networks essentially have no clustering, unlike the two null models, suggesting that the lack of clustering is a unique characteristic of the evolved networks. Finally Figure 2(d) shows the evolved networks to be highly disassortative. The degree of disassortativity displayed by the evolved networks is similar to the level of disassortativity found in the degree randomized model, indicating that the disassortativity is a consequence of the degree distribution. In short, the degree distribution accounts for the path-length characteristics and assortativity in the evolved networks, while the degree of clustering is a unique property of the evolved networks.

Figure 3 shows a comparison between networks with enhanced instability properties and the two null models.

FIGURE 4: Degree distributions. (a) Degree distribution for networks with enhanced stability properties; (b) Degree distribution for networks with enhanced instability properties.

Figures 3(a), 3(b), and 3(c) show that the average shortest path-length, diameter, and clustering are significantly larger than those found in the two null models, suggesting that these characteristics are unique to the evolved class of networks. Combined, these characteristics indicate that these networks have the so-called “long-world” properties. Finally, these networks are assortative (Figure 3(d)), but it should be noted that the spread of these distributions is wide. The analysis suggests that the evolved networks are somewhat “unique” in their wiring which gives them topological properties which are not solely accounted for by the degree distribution.

Studies of many real-world networks have identified skewed degree distributions—particularly those whose distributions decay as a power-law—as a key characteristic [7]. Figure 4 shows the degree distribution for the networks with enhanced stability and instability properties compared to an Erdős-Rényi random graph. The degree distribution for networks with enhanced stability is heavily skewed. Despite the short tail (due to finite size effects), there is a significant fraction of nodes with large degrees. By contrast, the degree distribution for networks with enhanced instability is quite peaked, with a narrower variance than an Erdős-Rényi random graph. This suggests that networks with enhanced instability have a degree of regularity about the way links are distributed throughout the network.

5. RESILIENCE TO TOPOLOGICAL ATTACK

Now, we examine the topological stability [11] of the evolved networks. By topological stability, we mean how these networks break apart when nodes are removed from the network. Here, we consider two node removal schemes: (1) random node removal; and (2) degree centrality node removal. Under the random node removal scheme, nodes are

FIGURE 5: Decay of networks as nodes are randomly and targetedly removed from the network. Solid lines are networks with enhanced stability properties, and dashed lines are networks with enhanced instability properties.

removed from the network without bias. Under the degree centrality node removal scheme, nodes are removed based on their degree. After a node is removed from the network, the centrality of each node is recalculated. If two nodes have the same centrality score, the node selected to be removed from the network is chosen at random. To test topological stability of the evolved networks, we took 200 optimized networks from both optimization schemes and subjected each network to the aforementioned attack regimes. This was repeated 100 times for each network, to allow for adequate selection between tied centrality measures. As nodes were removed, we kept track of size of the largest connected component $\langle s \rangle$.

From Figure 5, we can see how the network's largest connected component $\langle s \rangle$ breaks-up as nodes are removed in accordance with the attack schemes. The most striking observation here is that networks with enhanced stability properties are highly fragile to targeted node removal, yet are highly resilient to random node removal. By optimizing for dynamic stability, topological stability to random attack is gained at no cost. By contrast, networks with enhanced instability properties are less resilient to random node removal than networks with enhanced stability properties, but these networks are more resilient to targeted node removal. The networks described here appear to have the same degree sequence as those studied in [12–15]. However, it is not clear if those networks possess the stability properties of the networks described here. Our networks have a very specific set of topological properties that are not accounted for by the degree distribution alone (see Section 4).

6. DISCUSSION

In this paper, we have employed the use of a search algorithm to identify network characteristics that seem to be associated with enhanced linear stability and instability properties. Figure 1 shows that the optimized networks display a degree of structural regularity in their arrangement. Networks with enhanced stability properties take on a star-like structure. While finite size effects make it difficult to determine the exact role and configuration of hubs that make these networks more stable, we postulate that the hubs allow

perturbations to be distributed and reabsorbed quickly. We also make the following general observations about the networks with enhanced stability properties. Networks with enhanced stability properties (i) have very low clustering and almost no cycles, (ii) have a highly skewed degree distribution and the degree distribution accounts for many of the observed network characteristics, (iii) have short paths between any two nodes, a small diameter, and are highly disassortative, and (iv) are highly resilient to random attack, but highly sensitive to targeted attack. It is tempting to suggest that when a network is optimizing for stability, topological stability to random failure is obtained as a no-cost bonus.

By contrast we make quite different observations about the networks with enhanced instability properties. They (i) have an interlocked loop structure, (ii) have a peaked degree distribution, and the degree distribution is not the sole source of the structural properties observed within these networks, (iii) tend to have longer average shortest path-lengths, larger diameter, higher clustering, and tend to be more assortative than random null models, and (iv) are resilient to both random and targeted attacks.

In this paper, we have shown that the ability of small initial shocks to cascade to the extent that large systems are affected or disrupted is directly linked to the way the underlying system elements are connected [4]. Understanding the way a network is structured provides great insights into the dynamical properties demonstrated by that network [16, 17]. Many biological, social, and large-scale infrastructure networks display a surprising degree of similarity in their overall organization. For example, the frequency with which we observe scale-free networks in the real world may be explained by their demonstrated topological and dynamical stability. However, while these systems may look structurally similar, the origins of their similarity may be quite different. Biological networks, for example, exploit homeostasis provided by certain network properties, while technological networks arrive at the same properties as the result of a trade-off between communication efficiency and link cost [18]. From the simple system dynamics studied here, we suggest that large complex networks can be designed to be robust to perturbations, if simple structural design rules are followed.

REFERENCES

- [1] U.S.-Canada Power System Outage Task Force, “Final Report on the August 14th blackout in the United States and Canada,” <https://reports.energy.gov/BlackoutFinal-Web.pdf>.
- [2] J. Ash and D. Newth, “Optimizing complex networks for resilience against cascading failure,” *Physica A*, vol. 380, no. 1–2, pp. 673–683, 2007.
- [3] A. J. Lotka, *Elements of Physical Biology*, Williams & Wilkins, Baltimore, Md, USA, 1925.
- [4] R. M. May, *Stability and Complexity in Model Ecosystems*, Princeton University Press, Princeton, NJ, USA, 2001.
- [5] D. Newth and M. Brede, “Fitness landscape analysis and optimization of coupled oscillators,” *Complex Systems*, vol. 16, no. 4, pp. 317–331, 2006.
- [6] P. Erdős and A. Rényi, “On random graphs. I,” *Publicationes Mathematicae*, vol. 6, pp. 290–297, 1959.

- [7] R. Albert and A.-L. Barabási, “Statistical mechanics of complex networks,” *Reviews of Modern Physics*, vol. 74, no. 1, pp. 47–97, 2002.
- [8] D. J. Watts and S. H. Strogatz, “Collective dynamics of “small-world” networks,” *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.
- [9] M. E. J. Newman, “Detecting community structure in networks,” *The European Physical Journal B*, vol. 38, no. 2, pp. 321–330, 2004.
- [10] R. Milo, S. Shen-Orr, S. Itzkovitz, N. Kashtan, D. Chklovskii, and U. Alon, “Network motifs: simple building blocks of complex networks,” *Science*, vol. 298, no. 5594, pp. 824–827, 2002.
- [11] R. Albert, H. Jeong, and A.-L. Barabási, “Error and attack tolerance of complex networks,” *Nature*, vol. 406, no. 6794, pp. 378–382, 2000.
- [12] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, “Resilience of the Internet to random breakdowns,” *Physical Review Letters*, vol. 85, no. 21, pp. 4626–4628, 2000.
- [13] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, “Breakdown of the internet under intentional attack,” *Physical Review Letters*, vol. 86, no. 16, pp. 3682–3685, 2001.
- [14] T. Tanizawa, G. Paul, R. Cohen, S. Havlin, and H. E. Stanley, “Optimization of network robustness to waves of targeted and random attacks,” *Physical Review E*, vol. 71, no. 4, Article ID 047101, 4 pages, 2005.
- [15] T. Tanizawa, G. Paul, S. Havlin, and H. E. Stanley, “Optimization of the robustness of multimodal networks,” *Physical Review E*, vol. 74, no. 1, Article ID 016125, 8 pages, 2006.
- [16] S. H. Strogatz, “Exploring complex networks,” *Nature*, vol. 410, no. 6825, pp. 268–276, 2001.
- [17] D. J. Watts, “A simple model of global cascades on random networks,” *Proceedings of the National Academy of Sciences of the United States of America*, vol. 99, no. 9, pp. 5766–5771, 2002.
- [18] R. V. Solé, R. Ferrer-Cancho, J. M. Montoya, and S. Valverde, “Selection, tinkering, and emergence in complex networks,” *Complexity*, vol. 8, no. 1, pp. 20–33, 2003.