IEICE Proceeding Series

Analytical Approach to the Robustness of Strongly Correlated Complex Networks

Toshihiro Tanizawa, Shlomo Havlin, H. Eugene Stanley

Vol. 1 pp. 102-105
Publication Date: 2014/03/17
Online ISSN: 2188-5079

2012 International Symposium on Nonlinear Theory and its Applications
NOLTA2012, Palma, Majorca, Spain, October 22-26, 2012

Analytical Approach to the Robustness of Strongly Correlated Complex Networks

Toshihiro Tanizawa†, Shlomo Havlin‡, and H. Eugene Stanley*

†Kochi National College of Technology
200-1 Monobe-Otsu, Nankoku, Kochi, 783-8508, Japan
‡Minerva Center and Department of Physics,
Bar-Ilan University, 52900 Ramat-Gan, Israel
* Center for Polymer Studies and Department of Physics,
Boston University, Boston, MA 02215, USA
Email: tanizawa@ee.kochi-ct.ac.jp, havlin@ophir.ph.biu.ac.il, hes@bu.edu

Abstract—The robustness of complex networks against external perturbations, such as node and/or link removal, is critical for the functioning of a complex network and has been studied through various approaches. Most analytical work assumes, for simplicity, that there is no specific correlation in connecting nodes, because of the difficulty and complexity in treating correlation between node connections properly. Since many networks in the real world do have such correlation, we focus on deriving analytical equations for calculating the threshold and the giant component fraction for networks having degree-degree correlations against arbitrary strategies of node removal. As an example of the analyses using these expressions, we show how the vulnerability of scale-free networks against targeted node removal can be significantly improved by taking the structure in which the nodes with almost the same degree are connected to each other. Our analytic calculations are verified by numerical simulations.

1. Introduction

Many complex systems in real world can be modeled by complex networks. Generally speaking, the cooperative performance of complex systems fundamentally relies on the global connectivity of their components. These complicated systems are, however, usually placed in an ever-changing external environment where the components or the connections could be constantly added, eliminated, or changed. Such changes may potentially affect the global connectivity of the network under consideration to the extent in which the global connectivity could be completely lost and the system represented by the network will lose its functionality. The analysis of the response of the global connectivity caused by the alteration of the network, or targeted attacks, has been therefore one of the main issues of the complex network analysis. Most of the existing theoretical studies on the robustness of complex networks, however, depend only on the degree distribution

Recently, Schneider et al. developed an interesting numerical approach for enhancing network robustness against high degree node removal [6, 7]. They start from an uncorrelated random network with a given degree distribution. Next, they randomly choose two pairs of links and exchange the destinations of the two links between them keeping the overall degree distribution unchanged. If this exchange improves the robustness of the network against targeted node removal, the exchange is accepted. By repeating this procedure, the robustness of the network is enhanced step by step. They applied this method to several types of networks with broad degree distributions and found that the final robust networks have a common "onion-like" topology consisting of a core of highly connected nodes hierarchically surrounded by rings of nodes with decreasing degree [6, 7]. In each ring most of the nodes are of the same degree.

Motivated by the onion-like topology, we study here analytically the robustness of a family of such systems [8]. In our approach we obtain analytical expressions for the critical threshold and for the giant components, where the degree-degree correlation is fully incorporated. Due to the analytical approach, a statistical treatment over large number of realizations as done in computer simulations is not needed to obtain definite results. Nevertheless both analytical and simulation approaches are necessary and complementary, in particular, for testing the analytical approach. Interestingly, the optimal structure we find here against simultaneous random and targeted high degree node removals is very similar to the "onion-like" structure found by Schneider et al. [7]. The optimal structure obtained consists of hierarchically and weakly interconnected random regular graphs.

2. Theory

We start from the joint degree-degree probability matrix, $P(k, k')$, which is the probability that a randomly chosen link emanates from a k-degree node and ends at a k'-degree node. In this article, we consider only the cases of undirected networks, where the symmetry $P(k, k') = P(k', k)$ holds. The sum of $P(k, k')$ over k' is the probability that a randomly chosen link starts from a k-degree node. It is related to the probability density of the degree distribution, $P(k)$, through the relation, $\sum_{k'} P(k,k') = kP(k)/\langle k\rangle$, where $\langle k\rangle$ is the average degree. By definition, $\sum_k P(k) = 1$. Note that the sum $\sum_{k'} P(k,k')$ has to be fixed if we fix the degree distribution, $P(k)$. The conditional probability, $P(k'|k)$, that a randomly chosen link emanating from a k-degree node leads to a k'-degree node is defined by $P(k'|k) \equiv P(k,k')/\sum_{k'} P(k,k') = P(k,k')/\left(kP(k)/\langle k\rangle\right)$.

When the nodes of a network are removed according to the degree of nodes, the remaining fraction of k-degree nodes is reduced by a factor b_k ($0 \le b_k \le 1$) from the original fraction, $P(k)$. The total remaining fraction of nodes, p, is calculated as $p = \sum_k b_k P(k)$.

The giant component in a complex network is a cluster of connected nodes, where its normalized size in the network, S, remains finite as the total number of nodes, N, becomes infinite. Non-zero values of S indicate a macroscopic connectivity of the network under consideration.

To calculate the critical value of the remaining fraction of nodes, p_c, above which the giant component, S, begins to take a non-zero value, we extend the generating function method [2, 5] by incorporating the degree-degree correlation under an arbitrary type of degree based node removal. Let x_k be the probability that a randomly chosen link from a k-degree node does not lead to the giant component. We assume that the network only consists of trees, which is justified in the limit of $N \to \infty$. The probabilities, x_k, $(k = m, m+1, \ldots, K)$, for non-zero values of b_k is determined by the following self-consistent equations for each k:

$$x_k = \sum_{k'}(1 - b_{k'})P(k'|k) + \sum_{k'} b_{k'}P(k'|k)\,(x_{k'})^{k'-1}. \qquad (1)$$

Using these x_k's, the probability that a randomly chosen node does not belong to the giant component fraction, which is $1 - S$, is determined by the equation,

$$1 - S = \sum_k (1 - b_k)P(k) + \sum_k b_k P(k)(x_k)^k. \qquad (2)$$

These equations are diagrammatically represented in Fig. 1. From Eq. (2), the giant component fraction, S, is obtained by the equation,

$$S = p - \sum_k b_k P(k)\,(x_k)^k = \sum_k b_k P(k)\left(1 - (x_k)^k\right), \qquad (3)$$

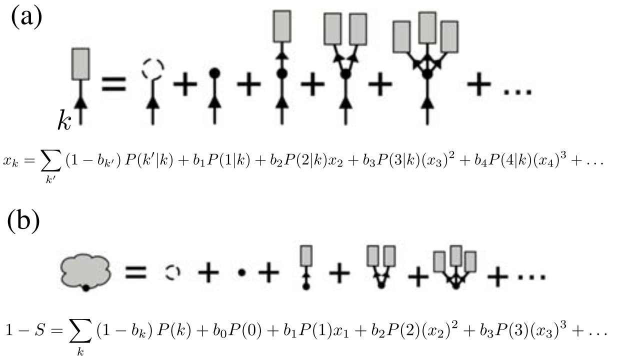
where $p = \sum_k b_k P(k)$ is the total remaining node fraction.

Obviously, $x_k = 1$ for removing all k-degree nodes ($b_k = 0$). Note that these equations contain the remaining fraction of k-degree nodes, b_k. Equations (1) and (3) are a necessary extension of existing works in order to investigate all types of node removal. The degree-degree correlation is included in the conditional probability, $P(k'|k)$.

Below the critical remaining fraction of nodes, all x_k's are equal to one and it follows from Eq. (3) that $S = 0$ (no giant component). At criticality where the giant component emerges, at least one of x_k's takes a value slightly smaller than one. In the vicinity of the critical point, we assume $x_k = 1 - y_k$ and expand Eq. (1) in terms of infinitesimally positive quantities y_k. The equation obtained by this expansion becomes

$$y_k = \sum_{k'} B_{kk'} y_{k'} + O(y_k^2), \qquad (4)$$

where the "branching matrix," $B_{kk'}$, is defined by $B_{kk'} \equiv b_{k'}P(k'|k)(k'-1)$. The eigenvalues of the branching matrix are all non-negative and can be ordered according to their values. The critical point can be obtained by the point at which the largest eigenvalue of $B_{kk'}$ becomes unity [5].



$$x_k = \sum_{k'} (1 - b_{k'})\,P(k'|k) + b_1 P(1|k) + b_2 P(2|k) x_2 + b_3 P(3|k)(x_3)^2 + b_4 P(4|k)(x_4)^3 + \ldots$$

$$1 - S = \sum_k (1 - b_k)\,P(k) + b_0 P(0) + b_1 P(1) x_1 + b_2 P(2)(x_2)^2 + b_3 P(3)(x_3)^3 + \ldots$$

Figure 1: Diagrammatic representation of the equations that determine x_k and S. The diagram (a) represents the equation for the probability x_k and the diagram (b) represents the equation for the probability that a randomly chosen node does not belong to the giant component, which is $1 - S$. The dashed line circles represent that the k-degree nodes are vacant by removal with probability $1 - b_k$.

3. Optimal Structure

The robustness of a given network depends on the method of node removal. For example, scale-free networks are almost completely robust against random node removal while they are extremely vulnerable against targeted removal of high degree nodes [1, 2, 3, 4]. The results for the robustness is, however, derived for random networks and thus are based only on the degree distribution. It is interesting, therefore, to clarify to what extent we are able to improve the robustness of a complex network against targeted attack by introducing the degree-degree correlation while keeping the network degree distribution unchanged.

With this in mind, we focus on the improvement of the robustness of complex networks against targeted high degree node attack. We limit our analysis to networks where the number of k-degree nodes decreases with increasing k. In targeted high degree attack, all nodes that have higher degrees than a certain value are eliminated. Removing a node also eliminates all the edges attached to it.

Since the edges are connected with the remaining lower degree nodes, the elimination of those edges undermines the global connectivity of the remaining lower degree node component. In order to minimize such undermining effects as much as possible, the number of edges that connect removed higher degree nodes and the remaining lower degree nodes should be minimized as much as possible. Hence the following requirement should be fulfilled.

Requirement: The k-degree nodes should not be connected to nodes with degree, k', lower than k ($k' < k$).

This Requirement yields that most of the edges should connect nodes of the same degree. Thus the optimal structure built up from a set of random regular (RR) graphs naturally emerges. To form an entirely connected single network, these RR graphs must be connected with one another. The most robust network against targeted attack with a given degree distribution can, therefore, be constructed by the following procedure.

1. Prepare a suitable number of nodes for each degree according to the given degree distribution. We assume that the number of nodes for each degree is so large that all edges can find nodes to be attached in both end points.

2. Let the smallest degree be m and begin to construct the network from an m-degree component, which is the last remaining component for targeted high degree node removal. If the Requirement is completely fulfilled, no edges of the m-degree component are eliminated by targeted removal of nodes with degree larger than but not equal to m. The last remaining m-degree component forms, therefore, an RR graph of degree m.

3. Next, attach the nodes with degree $m + 1$. According to the Requirement, the attached $(m + 1)$-degree nodes cannot be connected to the (smaller) m-degree component. Thus all $(m + 1)$-degree nodes should be connected with one-another and forms an RR graph of degree $(m + 1)$.

   Up to this point, the network consists of two separated RR graphs with degree m and $m+1$. However, to make a single connected network we have to connect these two components. To fulfill the Requirement as much as possible under the condition of the fixed degree distribution, we break two edges, the one of which is in the RR graph of degree m and the other of which is in the RR graph of degree $m + 1$, and rewire these two edges. Note that this rewiring does not change the degree distribution.

4. Attaching the nodes with next larger degree, $m+2$ can be performed in the same way. First, following the Requirement, these nodes should be connected with one-another. Hence, an RR graph with degree $m + 2$ emerges. Next, to make a single connected network under the conditions of the Requirement and the fixed degree distribution, two edges in the RR graph of degree $m+1$ and the RR graph of degree $m+2$ are broken and rewired.

   By repeating this argument up to the nodes with the largest degree, K, we reach the structure in which RR graphs with degrees hierarchically up from m to K are minimally interconnected. This structure has a close resemblance with the robust "onion-like" structure found using numerical simulations by Schneider et al. [6, 7].

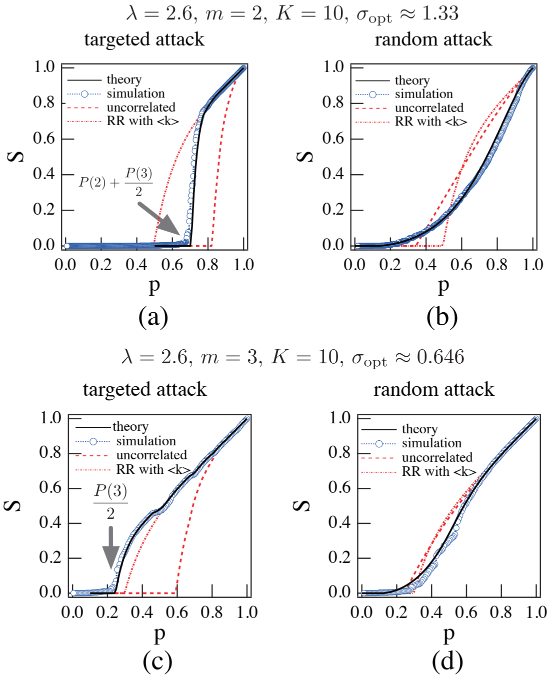


Figure 2: (Color online) Plots of the giant component, S, of scale-free networks with $\lambda = 2.6$ and $K = 10$ of the optimal structure proposed in Section 3 as a function of p. For plots (a) targeted attack and (b) random attack, we set $m = 2$ and for plots (c) targeted attack and (d) random attack, $m = 3$. In all plots, the theoretical values for the giant component are represented by full curves. The critical node thresholds for targeted attack are $P(2) + P(3)/2$ for $m = 2$ and $P(3)/2$ for $m = 3$. We also plot, for comparison, the curves for the corresponding uncorrelated scale-free network with the same values of parameters (dashed curves) and for the RR network with the same degree as the average degree of the corresponding scale-free network (dotted curves). The (blue) circles are obtained from simulation of a single realization for each of the optimal networks with the total nodes, $N = 6993$ for $m = 2$ and with $N = 2795$ for $m = 3$.

4. Results

In Fig. 2, we plot the giant components of scale-free networks for targeted and random attacks, in which the degree distribution is represented by $P(k) \propto k^{-\lambda}$, constructed by the procedure described in Section 3 as a function of the remaining fraction of nodes, p. In these plots, we set the exponent, $\lambda = 2.6$, and the maximum degree, $K = 10$. Two values of the minimum degree, $m = 2$ and $m = 3$, are calculated. The theoretical values of the giant component fraction are represented by full curves. The critical node thresholds for targeted attack are $P(2) + P(3)/2$ for $m = 2$ and $P(3)/2$ for $m = 3$, respectively. For comparison, we also plot the curves for the corresponding uncorrelated scale-free network with the same parameters and for the RR network of the same degree as the average degree of the corresponding scale-free networks. These results show that the robustness of scale-free networks against targeted attack can be significantly improved up to nearly maximal by taking the structure of weakly interconnected RR graphs (onion-like structures) without much undermining their intrinsic robustness against random failure.

For testing our theoretical considerations, we also simulate actual networks corresponding to the ones theoretically calculated. The circles in Fig. 2 are obtained by direct node removal from the simulated optimal networks. For each realization, the number of nodes for $m = 2$ is 6993 and for $m = 3$ is 2795. The agreement between the simulation results and the theoretical calculations is excellent.

5. Summary

As a strong candidate for the optimal structure against both types of attacks, random and targeted, with a given degree distribution, the structure consisting of hierarchically interconnected random regular graphs is proposed and thoroughly investigated based on exact analytical expressions. This network structure has a close relationship with the "onion-like structure" found by Schneider et al. [6, 7] using numerical simulations and exhibits an extremely assortative degree-degree correlation, in which a node of certain degree has a strong tendency to be linked with nodes of the same degree. We derive a set of exact expressions that enable us to calculate the critical node threshold and the giant component fraction for arbitrary types of node removal, in which the degree-degree correlation is fully incorporated. To test the robustness of this structure, we apply the theory to the case of scale-free networks that have a well-known vulnerability against targeted attack. The results show that the vulnerability of a scale-free network can be significantly improved by taking the network structure proposed here without much undermining its almost complete robustness against random attack. We also investigate the detail of the robustness enhancement of scale-free networks due to assortative degree-degree correlation by introducing a joint degree-degree probability matrix that interpolates between an uncorrelated network structure and the structure with strong assortativity by tuning a single control parameter. The optimal values of the control parameter that maximize the robustness against simultaneous random and targeted attacks are also determined and those optimal values support the maximal robustness of the "onion-like structure." Our analytical calculations are supported by numerical simulations.

Acknowledgments

This work is supported by the Grant-In-Aid for Scientific Research (C) from the Japan Society for the Promotion of Science, No. 20540382 and No. 24540419. We also wish to thank the ONR, DTRA, DFG, EU project Epiwork, the LINC EU project, NSF and the Israel Science Foundation for financial support.

References

[1] R. Albert, H. Jeong, and A.-L. Barabási. Error and attack tolerance of complex networks. *Nature (London)*, 406:378–382, Feb 2000.

[2] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts. Network Robustness and Fragility: Percolation on Random Graphs. *Phys. Rev. Lett.*, 85:5468–5471, Dec. 2000.

[3] R. Cohen, K. Erez, D. ben Avraham, and S. Havlin. Resilience of the Internet to Random Breakdowns. *Phys. Rev. Lett.*, 85(21):4626–4628, Nov. 2000.

[4] R. Cohen, K. Erez, D. ben Avraham, and S. Havlin. Breakdown of the Internet under Intentional Attack. *Phys. Rev. Lett.*, 86(16):3682–3685, Apr. 2001.

[5] A. V. Goltsev, S. N. Dorogovtsev, and J. F. F. Mendes. Percolation on correlated networks. *Phys. Rev. E*, 78(5):051105, Nov. 2008.

[6] H. J. Herrmann, C. M. Schneider, A. A. Moreira, J. S. Andrade Jr, and S. Havlin. Onion-like network topology enhances robustness against malicious attacks. *Journal of Statistical Mechanics: Theory and Experiment*, 2011(01):P01027, Jan. 2011.

[7] C. M. Schneider, A. A. Moreira, J. S. Andrade Jr, S. Havlin, and H. J. Herrmann. Mitigation of malicious attacks on networks. *PNAS*, 108(10):3838–3841, Feb. 2011.

[8] T. Tanizawa, S. Havlin, and H. E. Stanley. Robustness of onion-like correlated networks against targeted attacks. *Phys. Rev. E*, 85(4):046109, Mar. 2012.