Invited Paper

Structural robustness and transport efficiency of complex networks with degree correlation

Toshihiro Tanizawa^{1 a)}

¹ *Kochi National College of Technology*

200-1 Monobe-Otsu, Nankoku, Kochi 783-8508, Japan

^{a)} *tanizawa@ee.kochi-ct.ac.jp*

Received July 31, 2012; Revised September 26, 2012; Published April 1, 2013

Abstract: We examine two properties of complex networks, the robustness against targeted node removal (attack) and the transport efficiency in terms of degree correlation in node connection by numerical evaluation of exact analytic expressions. We find that, while the assortative correlation enhances the structural robustness against attack, the disassortative correlation significantly improves the transport efficiency of the network under consideration. This finding might shed light on the reason why some networks in the real world prefer assortative correlation and others prefer disassortative one.

Key Words: complex networks, correlation, robustness, targeted attack, transport

1. Introduction

Many complex systems in the real world can be modeled by complex networks [1–11]. The cooperative performance of such complex systems relies on the global connectivity of their components. These complex systems are placed, however, in an external environment, where the components or connections could be removed and/or altered. The analysis of the response of the global connectivity caused by intentional node removal of the network, or targeted attacks, has been, therefore, one of the main issues of the complex network analysis [5–31].

Although most of the existing theoretical studies on robustness analysis of complex networks are based on arguments based only on the degree distribution, the effects of degree correlation between node connection begin to be considered recently [32–36]. In the early stage of complex network research, however, Newman already argued that networks in the real world exhibit rather strong tendency, or correlation, in the connection between nodes of different degrees [37]. He introduced the terms, assortative and disassortative correlations, to describe the tendency of nodes in a network to make connections between the same degree and between different degrees, respectively. Social networks, such as friendship relations, collaboration networks in scientific research, and so on, tend to be assortative, and communication networks, such as WWW, neural networks, autonomous system networks on the Internet, and so on, tend to be disassortative. Newman also calculated the giant component collapse for specific kinds of correlated networks against random node removal and found that

assortativity enhances the robustness of networks against random attack. Goltsev et al. focused on the evaluation of critical exponents of correlated complex networks in the vicinity of node percolation transition for the case of random attack [33].

Regarding to a robustness analysis against targeted attack, Schneider et al. numerically found that the final robust network structure have a common “onion-like” topology consisting of a core of highly connected nodes hierarchically surrounded by rings of nodes with decreasing degree [38, 39]. In each ring most of the nodes are of the same degree. Tanizawa et al. took an analytic approach to the robustness analysis against targeted attack [36]. Interestingly, they found that the optimal structure against simultaneous random and targeted attack is very similar to the “onion-like” structure found by Schneider et al. The optimal structure obtained consists of hierarchically and weakly interconnected random regular graphs and exhibits extremely assortative degree correlation.

With respect to the structural robustness against targeted attack, assortative degree correlation is favorable. However, there are considerable number of functional complex networks in the real world that show disassortative degree correlation, such as WWW, neural networks, autonomous system networks on the Internet. Within the author’s knowledge, there seems to be no plausible argument for the emergence of disassortative networks. When we consider that most of the networks that exhibit disassortativity are communication oriented, in other words, that the primary function of these networks is information exchange, it is likely that the efficiency of the information exchange dominates in determining their network structure. Gallos et al. considered the effects of degree correlation in terms of fractality in network structure and argued the particle diffusion is accelerated on the network structure with strong hub repulsion [40].

In this paper, we examine the robustness against targeted attack and the transport efficiency of complex networks in terms of assortative (disassortative) degree correlation by numerical evaluation of exact analytic expressions, expecting that the results shed some light on the reason of the emergence of assortativity (disassortativity) in various complex networks in the real world.

This paper is organized as follows. In Sec. 2, we describe the theoretical framework for the calculation of the robustness and the transport efficiency of complex networks with degree correlation under the condition of fixed degree distribution. In Sec. 3, we show the results of the calculation based on the theory described in Sec. 2. There we see that the disassortativity enhances the transport efficiency, while the assortativity enhances the structural robustness against targeted attack. Section 4 is for discussion and summary.

2. Theory

2.1 Degree distribution and degree correlation

Since we consider the degree correlation in node connection, we start from the joint degree matrix, $P(k, q)$, which is the probability that a randomly chosen edge from a k -degree node leads to a q -degree node. For undirected networks, the symmetry $P(k, q) = P(q, k)$ holds. The sum of $P(k, q)$ over q is the probability that a randomly chosen edge emanates from a k -degree node and is related to the degree distribution, $P(k)$, with the normalization condition, $\sum_k P(k) = 1$, through the relation, $\sum_q P(k, q) = kP(k)/\langle k \rangle$, where $\langle k \rangle = \sum_k kP(k)$ is the average degree. By definition, $\sum_{k,q} P(k, q) = 1$. If we fix the degree distribution, $P(k)$, the sum, $\sum_q P(k, q)$, has also to be fixed.

The conditional probability, $P(q|k)$, that a randomly chosen edge from a k -degree node leads to a q -degree node, which is defined by $P(q|k) \equiv P(k, q)/\sum_q P(k, q) = P(k, q)/(kP(k)/\langle k \rangle)$, contains the information of the degree correlation of the network under consideration. This conditional probability, $P(q|k)$, is normalized for each k as $\sum_q P(q|k) = 1$. For networks without degree correlation, $P(q|k)$ is independent of k and equals to $qP(q)/\langle k \rangle$. This means that the joint degree matrix for uncorrelated networks is separable and becomes $P(k, q) = (kP(k)/\langle k \rangle)(qP(q)/\langle k \rangle)$.

Although the theoretical framework taken in this paper is generic and applicable to any form of joint degree matrices, $P(k, q)$, we here consider the cases of scale-free networks where the degree distribution takes a power-law form, $P(k) \propto k^{-\lambda}$ ($k = m, m+1, \dots, K-1, K$). Here we denote the minimum degree as m and the maximum degree as K . In these cases, the joint degree matrix is finite

and the degree dependence of its matrix elements for uncorrelated (scale-free) networks is represented by $P_0(k, q) \sim k^{1-\lambda} q^{1-\lambda}$. By modifying the degree dependence of the joint degree matrix from this uncorrelated one, we can introduce the degree correlation. Note that, because of the symmetry of $P(k, q)$ in terms of k and q , we are only allowed to determine the degree dependence of $P(k, q)$ for the elements corresponding to $q \geq k$. The matrix elements for $q < k$ are determined from the symmetry and the normalization condition of $P(k, q)$.

If $P(k, q)$ decreases slower than $P_0(k, q)$ as q increases, the tendency of nodes to make connection with nodes of larger degree is enhanced. In this case, nodes are likely to be connected to large degree nodes ($q \gg k$). Thus the correlation is disassortative. In contrast, if $P(k, q)$ decreases faster than $P_0(k, q)$ as q increases, the tendency of nodes to make connection with nodes of larger degrees becomes smaller. In this case, nodes are more likely to be connected to nodes of similar degrees ($q \approx k$). Thus the correlation is assortative.

There are many possibilities to introduce degree correlation. Here we adopt a simple modification of the joint degree matrix, which is

$$P(k, q) \sim k^{1-\lambda} q^{1-\lambda+\epsilon} \quad (q \geq k). \quad (1)$$

This modification leads to the conditional probability in the form ¹

$$P(q|k) \sim q^{1-\lambda+\epsilon} \quad (q \geq k). \quad (2)$$

In this modification the degree correlation is controlled by a single parameter ϵ , which makes analysis sufficiently simple and mathematically tractable. Since $\epsilon = 0$ means the absence of degree correlation, nonzero values of ϵ indicate the existence of degree correlation. For $\epsilon > 0$, the values of $P(q|k)$ for larger q 's increase from the values of the uncorrelated networks ($\epsilon = 0$), which implies that the tendency of small degree nodes making connections with large degree nodes is enhanced. Thus $\epsilon > 0$ represents disassortative degree correlation. Similarly, $\epsilon < 0$ represents assortative degree correlation.

2.2 Giant component collapse due to attack

In targeted attack, where the nodes of a network are removed according to the degree of nodes, the remaining fraction of k -degree nodes is reduced to a factor b_k ($0 \leq b_k \leq 1$) 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 the largest 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. The resiliency of S under attack is taken to be a measure of the robustness of the network.

To calculate the giant component fraction, S , under degree correlation, we take the generating function formalism [16, 33, 36]. Let x_k be the probability that a randomly chosen link from a k -degree node does not lead to the giant component. In the limit of $N \rightarrow \infty$, the probability that a node is connected to any node that has already been connected to other nodes is negligible, since it is proportional to some negative power of N . Under the condition that the network only consists of trees, the probabilities, x_k ($k = m, m+1, \dots, K$), for non-zero values of b_k , and the node fraction of the giant component, S , are determined by the following set of equations:

$$x_k = 1 - \sum_q b_q P(q|k) + \sum_q b_q P(q|k) (x_q)^{q-1} \quad (3)$$

$$S = p - \sum_k b_k P(k) (x_k)^k = \sum_k b_k P(k) (1 - (x_k)^k). \quad (4)$$

Obviously, $x_k = 1$, if all k -degree nodes are removed ($b_k = 0$). The degree correlation is included in the conditional probability, $P(q|k)$. Although Eqs. (3) and (4) contain b_k and can be applicable to any types of degree based node removal, we focus on two simple types of attack in this paper: (i) targeted attack, which is the selective removal of nodes from the largest degree, and (ii) random attack, which is the uniform removal of nodes with equal probability.

¹Gallos et al. took a similar form for the joint degree probability [40]. It should be noted, however, that they gave the definition for $q \leq k$ and the definition of ϵ is different.

2.3 Diffusion on correlated networks

To investigate the transport property on complex networks with degree correlation, we consider a simple diffusion process described by the following simple diffusion equation:²

$$\frac{d}{dt}\rho_k(t) = -\rho_k(t) + k \sum_q P(q|k) \frac{\rho_q(t)}{q}, \quad (5)$$

where $\rho_k(t)$ is the density of “particles” on a randomly selected k -degree node at time t .

The first term in the right hand side of Eq. (5) represents the diffusion from the selected k -degree node and the second term represents the total in-coming flow from the q -degree neighbor nodes through its k edges. We assume that the “particles” flow out of a k -degree node through all of its edges with equal probability.

By taking vector notation as $\boldsymbol{\rho}(t) = \{\rho_m(t), \rho_{m+1}(t), \dots, \rho_{K-1}(t), \rho_K(t)\}$ and introducing the conditional probability matrix, $C = \{C_{kq}\} = kP(q|k)/q$, Eq. (5) can be simply represented as

$$\frac{d}{dt}\boldsymbol{\rho}(t) = -(\mathbf{I} - C)\boldsymbol{\rho}(t), \quad (6)$$

where $\mathbf{I}$ is the identity matrix. By the standard diagonalization procedure, the diffusion equations for each degree are reorganized to form a set of decoupled independent diffusion equations for each diffusive “mode”. The eigenvalues of the matrix $\mathbf{I} - C$, which are all non negative in the calculation presented in this paper, can be interpreted as the diffusion constants for these diffusive modes. The inverse of the largest positive eigenvalue, which we denote as μ , is the smallest characteristic time, $T = 1/\mu$, for these diffusive modes and serves as a good measure for evaluating the efficiency of the diffusion. Small values of T imply that particles on nodes diffuse in short time intervals, which we interpret as transport efficiency of the network under consideration.

3. Results

In this section, we present the results of calculation based on the theory described in the previous section for scale-free networks with the minimum degree $m = 2$, the maximum degree $K = 20$, and the exponent in the degree distribution, $\lambda = 1.0$.³

3.1 Giant component collapse

The existence of the giant component implies that the global connectivity in a network is maintained. As the total remaining node fraction, p , decreases, the node fraction belonging to the giant component, S , also decreases. Vanishing S means that the global connectivity is lost and a network is disintegrated. It is well known that S vanishes at a certain value of p , the threshold, by percolation phase transition. The value of the threshold depends on the structure of the network and the way of node removal.

For targeted attack, the parameters b_k in Eqs. (3) and (4) are taken to be

$$b_k = \begin{cases} 1 & (m \leq k < \tilde{K}), \\ b & (k = \tilde{K}), \\ 0 & (\tilde{K} < k \leq K), \end{cases} \quad (7)$$

where $\tilde{K}$ is the maximum degree of partially remaining nodes. The values of $\tilde{K}$ and b are determined by the total remaining node fraction through $p = \sum_{k=m}^{\tilde{K}} b_k P(k)$. For random attack, the node removal is uniform and all b_k ’s are equal to the total remaining node fraction, p .

In Fig. 1, we plot the giant component fraction S of scale-free networks with $m = 2$, $K = 20$, and $\lambda = 1.0$ as a function of the remaining node fraction, p , for various values of ϵ from $\epsilon = -1.0$

²This is the same equation that Gallos et al. examined in a different way [40].

³It is well known that λ takes a value between 2 and 3 for many scale-free networks in the real world. Since the main focus of this paper is to investigate the effects of disassortativity, we take $\lambda = 1.0$ in this paper to make the number of hubs larger and the effects of disassortativity much more prominent. We also calculated for the case of scale-free networks with $m = 2$, $K = 20$, and $\lambda = 2.2$ and obtained similar results.

Fig. 1. (Color online) Plots of the giant component fraction, S , as a function of remaining node fraction, p , for scale-free networks with $m = 2$, $K = 20$, and $\lambda = 1.0$ that have different values of ϵ from $\epsilon = -1.0$ (assortative, in blue) to $\epsilon = 0.4$ (disassortative, in red) through $\epsilon = 0$ (no correlation, in black). The plot (a) shows the giant component collapse due to targeted attack and the plot (b) shows the giant component collapse due to random attack. Note that, while the degree correlation plays no role in the case of random attack, the assortative (disassortative) degree correlation enhances (reduces) the resiliency of the giant component.

(assortative) to $\epsilon = 0.4$ (disassortative) through $\epsilon = 0$ (no correlation) against targeted attack and random attack. We see from Fig. 1(b) that the degree correlation plays almost no role in random attack. In contrast, the degree correlation significantly affects the decrease of S against targeted attack (Fig. 1(a)). As the assortativity becomes stronger ($\epsilon < 0$), the steep drop in S takes place at smaller values of p . Introducing assortative degree correlation thus makes a network more resilient against targeted attack.

As discussed in [36, 38, 39], the giant component begins to collapse faster for random attack as the assortativity sets in, while the remaining node threshold decreases slightly with the increase of assortativity. Therefore, the remaining node threshold does not serve as a good measure for the robustness. To compare the robustness against attack in terms of degree correlation, we take the area under the decreasing curve of S as the robustness measure, which represents the resiliency of the giant component due to node removal much more properly.⁴ (See the inset of Fig. 2.) We plot the robustness measure, R , calculated from the curves of S against targeted attack as a function of ϵ in Fig. 2. As the value of ϵ increases from -1.0 (assortative) to 0.4 (disassortative), the robustness measure, R , decreases almost linearly, which implies the scale-free network becomes more vulnerable against targeted attack as the degree correlation tends to disassortative. If the robustness against targeted attack is the first priority in designing network structure, the degree correlation should be assortative.

3.2 Transport efficiency

Networks in the real world are not static objects. There are flows of material, energy, information on the networks. The transport efficiency of these flows, as well as the structural robustness, should also be one of the crucial functionalities of complex networks.

To draw an overall picture of transport efficiency with respect to degree correlation, we examine the simple diffusion equation, Eq. (5), described in the previous section.

⁴This measure is the same as those used in [36, 38, 39]

Fig. 2. (Color online) Plot of the robustness measure, R , defined in the inset of the plot and calculated from the plot, Fig. 1(a) as a function of ϵ . As the value of ϵ increases from -1.0 (assortative) to 0.4 (disassortative), the robustness measure, R , decreases almost linearly, which implies the scale-free network becomes more vulnerable against targeted attack as the degree correlation tends to disassortative.

Fig. 3. (Color online) Plots of the time dependence of the density of diffusing particles on (a) a node of the minimum degree, m , and (b) a node of the maximum degree, K , in scale-free networks with $m = 2$, $K = 20$, and $\lambda = 1.0$ according to the diffusion equation, Eq. (6), under the initial condition that all particles are uniformly distributed on nodes of the minimum degree. Thus the particles diffuse from the smallest degree nodes to all the other larger degree nodes up to the maximum degree. Note that particles diffuse faster as the correlation parameter ϵ increases from -1.0 (assortative, in blue) to 0.4 (disassortative, in red).

In Fig. 3, we plot the densities of diffusing particles on a node of the minimum degree and a node of the maximum degree in scale-free networks with $m = 2$, $K = 20$, and $\lambda = 1.0$ as a function of time, t . In this calculation, all the particles are uniformly distributed on the nodes of minimum degree.

Fig. 4. (Color online) Plots of the time dependence of the density of diffusing particles on (a) a node of the minimum degree, m , and (b) a node of the maximum degree, K , in scale-free networks with $m = 2$, $K = 20$, and $\lambda = 1.0$ according to the diffusion equation, Eq. (6), under the initial condition that all particles are uniformly distributed on nodes of the maximum degree. Thus the particles diffuse from the largest degree nodes to all the other smaller degree nodes down to the minimum degree. Note that particles diffuse faster as the correlation parameter ϵ increases from -1.0 (assortative, in blue) to 0.4 (disassortative, in red).

Thus the particles flow out of minimum degree nodes and diffuse to other nodes of larger degree. Figure 3(b) shows the increase of the density on a node of maximum degree. From this plot, we can see that the density reaches its maximum faster as the degree correlation becomes disassortative. This is because, in disassortative networks, the tendency of minimum degree nodes making connection to the maximum degree nodes is larger and that the particles on minimum degree nodes can easily diffuse to larger degree nodes through these connections.

In Fig. 4, we plot the same diffusion process except for the initial condition, in which all particles are uniformly distributed on nodes of maximum degree. Also in this case, the particles diffuse faster in disassortative networks.⁵

The inverse of the largest positive eigenvalues, μ , of the coefficient matrix, $I - C$, of the diffusion equation, Eq. (6), can be taken as a measure the characteristic diffusion time, $T(= 1/\mu)$, the behavior of which we plot in Fig. 5 as a function of ϵ . It is interesting that the decrease in T has a bend at $(\epsilon, T) = (0, 1)$ (no correlation) and gets steeper in disassortative region ($\epsilon > 0$). This means that the diffusion takes place much faster in disassortative networks. Thus the transport efficiency favors disassortative degree correlation.

4. Discussion and summary

Structural robustness and transport efficiency are both important qualities for the proper functioning of a complex network in the real world. From the results presented in this paper, we see that assortative correlation is favorable for structural robustness, whereas disassortative correlation is favorable for transport efficiency.

As Newman pointed out, both assortative and disassortative scale-free networks occur in the real world [37]. Social networks, such as friendship relations, collaboration networks in scientific research, and so on, tend to be assortative, and communication networks, such as WWW, neural networks,

⁵The density, $\rho_k(t)$, in the diffusion equation, Eq. (5), is the density of “particles” on each node. Since the number of nodes of m degree is much larger than the number of nodes of K degree in scale-free networks, the final values of ρ_m plotted in Fig. 4(a) are much smaller than the final values of ρ_K plotted in Fig. 3(b).

Fig. 5. (Color online) Plot of the characteristic time for diffusion, T , defined by the inverse of the largest positive eigenvalue, μ , of the coefficient matrix, $I - C$. As the value of ϵ increases from -1.0 (assortative) to 0.4 (disassortative), the characteristic time, T , decreases almost linearly with a bend at $(\epsilon, T) = (0, 1)$ (no correlation). The decreasing rate in T is much steeper in the disassortative region ($\epsilon > 0$) than that in the assortative region ($\epsilon < 0$).

autonomous system networks on the Internet, and so on, tend to be disassortative.

Within the author's knowledge, there is no plausible argument for the emergence of this difference. According to the results obtained here, one possible argument might be the following. If the required time scale of transport on a network for proper functioning is not so fast and the structural robustness against several types of attack is the first priority, the resulting network favors assortative degree correlation. In contrast, if the transport efficiency is crucial and mandatory, the resulting network favors disassortative degree correlation. The existing examples we have at present seem to fit this reasoning.

The results presented in this paper is, however, obtained from an application of the theory to very limited cases. To confirm the validity of the argument about the emergence of degree correlation, we need more extensive and thorough investigation, which will be open to our future work.

In summary, we examine the effect of degree correlation on structural robustness and transport efficiency of scale-free networks by numerical calculation based on exact analytic equations. The transport efficiency is significantly enhanced when the degree correlation becomes disassortative, whereas the structural robustness against targeted attack is improved as the assortative degree correlation becomes stronger. These opposite roles of degree correlation played in structural robustness and transport efficiency possibly provide a plausible argument for the emergence of various degree correlation in complex networks in the real world.

Acknowledgments

The author is grateful to Prof. Small and Prof. Nakamura for suggesting him to submit his work to NOLTA. He also thanks to the financial support of the Grant-in-Aid for Scientific Research (C) (No. 24540419).

References

- [1] D.J. Watts and S.H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature (London)*, vol. 393, pp. 440–442, May 1998.
- [2] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, pp. 509–512, October 1999.
- [3] R. Albert and A.-L. Barabási, "Statistical mechanics of complex networks," *Rev. Mod. Phys.*, vol. 74, pp. 47–97, January 2002.

- [4] M.E.J. Newman, “The structure and function of complex networks,” *SIAM Review*, vol. 45, pp. 167–256, June 2003.
- [5] S.N. Dorogovtsev and J.F.F. Mendes, *Evolution of Networks: From Biological Nets to the Internet and WWW*, Oxford University Press, New York, 2003.
- [6] R. Cohen, S. Havlin, and D. Ben-Avraham, *Structural Properties of Scale-Free Networks*, in *Handbook of Graphs and Networks: From the Genome to the Internet (Chapter 4)*. Weinheim, FRG: Wiley-VCH Verlag GmbH & Co. KGaA, 2005.
- [7] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang, “Complex networks: Structure and dynamics,” *Physics Reports*, vol. 424, pp. 175–308, 2006.
- [8] G. Calderelli and A. Vespignani, *Large Scale Structure and Dynamics of Complex Networks*, World Scientific, Singapore, 2007.
- [9] M.E.J. Newman, *Networks: An Introduction*, Oxford University Press, New York, 2010.
- [10] R. Cohen and S. Havlin, *Complex Networks: Structure, Robustness and Function*, Cambridge University Press, Cambridge, UK, 2010.
- [11] J. Gao, S. Buldyrev, S. Havlin, and H.E. Stanley, “Robustness of a network of networks,” *Phys. Rev. Lett.*, vol. 107, p. 195701, November 2011.
- [12] M. Molloy and B. Reed, “A critical point for random graphs with a given degree sequence,” *Random Structures & Algorithms*, vol. 6, pp. 161–180, March 1995.
- [13] R. Albert, H. Jeong, and A.-L. Barabási, “Error and attack tolerance of complex networks,” *Nature (London)*, vol. 406, pp. 378–382, February 2000.
- [14] R. Cohen, K. Erez, D. ben Avraham, and S. Havlin, “Resilience of the internet to random breakdowns,” *Phys. Rev. Lett.*, vol. 85, pp. 4626–4628, November 2000.
- [15] C. Moore and M.E.J. Newman, “Exact solution of site and bond percolation on small-world networks,” *Phys. Rev. E*, vol. 62, pp. 7059–7064, November 2000.
- [16] 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.*, vol. 85, pp. 5468–5471, December 2000.
- [17] R. Cohen, K. Erez, D. ben Avraham, and S. Havlin, “Breakdown of the internet under intentional attack,” *Phys. Rev. Lett.*, vol. 86, pp. 3682–3685, April 2001.
- [18] R. Cohen, D. ben Avraham, and S. Havlin, “Percolation critical exponents in scale-free networks,” *Phys. Rev. E*, vol. 66, p. 036113, September 2002.
- [19] F. Chung and L. Lu, “Connected components in random graphs with given expected degree Sequences,” *Annals of Combinatorics*, pp. 125–145, November 2002.
- [20] N. Schwartz, R. Cohen, D. ben Avraham, A.-L. Barabási, and S. Havlin, “Percolation in directed scale-free networks,” *Phys. Rev. E*, vol. 66, p. 015104, July 2002.
- [21] L.K. Gallos, R. Cohen, P. Argyrakis, A. Bunde, and S. Havlin, “Stability and topology of scale-free networks under attack and defense strategies,” *Phys. Rev. Lett.*, vol. 94, p. 188701, May 2005.
- [22] B. Shargel, H. Sayama, I.R. Epstein, and Y. Bar-Yam, “Optimization of robustness and connectivity in complex networks,” *Phys. Rev. Lett.*, vol. 90, p. 068701, February 2003.
- [23] A. Vázquez and Y. Moreno, “Resilience to damage of graphs with degree correlations,” *Phys. Rev. E*, vol. 67, no. 1, p. 015101, 2003.
- [24] G. Paul, T. Tanizawa, S. Havlin, and H.E. Stanley, “Optimization of robustness of complex networks,” *Eur. Phys. J. B*, vol. 38, pp. 187–191, May 2004.
- [25] T. Tanizawa, G. Paul, R. Cohen, S. Havlin, and H.E. Stanley, “Optimization of network robustness to waves of targeted and random attacks,” *Phys. Rev. E*, vol. 71, p. 047101, April 2005.
- [26] T. Tanizawa, G. Paul, S. Havlin, and H.E. Stanley, “Optimization of the robustness of multi-modal networks,” *Phys. Rev. E*, vol. 74, p. 016125, July 2006.
- [27] G. Paul, S. Sreenivasan, S. Havlin, and H.E. Stanley, “Optimization of network robustness to random breakdowns,” *Physica A*, vol. 370, pp. 854–862, August 2006.
- [28] L. Donetti, F. Neri, and M. Muñoz, “Optimal network topologies: expanders, cages, Ramanu-

- jan graphs, entangled networks and all that,” *Journal of Statistical Mechanics: Theory and Experiment*, p. P08007, August 2006.
- [29] G. Paul, R. Cohen, S. Sreenivasan, S. Havlin, and H.E. Stanley, “Graph partitioning induced phase transitions,” *Phys. Rev. Lett.*, vol. 99, p. 115701, September 2007.
 - [30] S.V. Buldyrev, R. Parshani, G. Paul, H.E. Stanley, and S. Havlin, “Catastrophic cascade of failures in interdependent networks,” *Nature (London)*, vol. 464, pp. 1025–1028, April 2010.
 - [31] X. Huang, J. Gao, S. Buldyrev, S. Havlin, and H.E. Stanley, “Robustness of interdependent networks under targeted attack,” *Phys. Rev. E*, vol. 83, June 2011.
 - [32] M.A. Serrano, M. Boguñá, and R. Pastor-Satorras, “Correlations in weighted networks,” *Phys. Rev. E*, vol. 74, p. 055101, November 2006.
 - [33] A.V. Goltsev, S.N. Dorogovtsev, and J.F.F. Mendes, “Percolation on correlated networks,” *Phys. Rev. E*, vol. 78, p. 051105, November 2008.
 - [34] Y. Shiraki and Y. Kabashima, “Cavity analysis on the robustness of random networks against targeted attacks: Influences of degree-degree correlations,” *Phys. Rev. E*, vol. 82, p. 036101, February 2010.
 - [35] M. Ostilli, A. Ferreira, and J. Mendes, “Critical behavior and correlations on scale-free small-world networks: Application to network design,” *Phys. Rev. E*, vol. 83, June 2011.
 - [36] T. Tanizawa, S. Havlin, and H.E. Stanley, “Robustness of onionlike correlated networks against targeted attacks,” *Phys. Rev. E*, vol. 85, p. 046109, April 2012.
 - [37] M.E.J. Newman, “Assortative Mixing in Networks,” *Phys. Rev. Lett.*, vol. 89, p. 208701, October 2002.
 - [38] C.M. Schneider, A.A. Moreira, J.S. Andrade Jr, S. Havlin, and H.J. Herrmann, “Mitigation of malicious attacks on networks,” *PNAS*, vol. 108, pp. 3838–3841, February 2011.
 - [39] 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*, vol. 2011, p. P01027, January 2011.
 - [40] L.K. Gallos, C. Song, and H.A. Makse, “Scaling of degree correlations and the influence on diffusion in scale-free networks,” *Phys. Rev. Lett.*, August 2008.