Annotated bibliography on complex networks

Jose M Sallan

1 Network models

The first attempt to model real-complex networks was the Erdös-Rényi (ER) model of random networks. That model does not represent adequately real-world networks.

As an explanation of real-world network being more clustered than random networks, Watts and Strogatz [24] defined the small-world property of complex networks: networks having this property have an average path length similar to random networks, but a much higher clustering coefficient. Later, Latora and colleagues [20] reformulated the small-world property in terms of global and local efficiency.

Barabási and colleagues introduced the BA scale-free model of complex networks, where the mechanisms of growth and preferential attachment lead to a degree distribution following a power law [4]. Arguably, the behavior of the world-wide-web can be explained with this model [5]. The BA model has a low clustering coefficient, contrarily to random networks, then in [18] is defined a KE generative model of highly-clustered scale-free networks.

Empirical research identified three structural classes of small-world networks: scale-free networks, with a degree distribution with a tail that decays as a power law, broad-scale or truncated scale-free, with a power-law regime followed by a sharper cutoff and single-scale networks, with a fast-decaying tail [2]. The emergence of the first two networks can be explained by optimization mechanisms, complementary to growth and preferential attachment [8].

2 Static robustness

Introduction of the problem of static robustness: [1].

Analysis of static robustness in terms of network efficiency: [12] for BA and KE graphs, [13] for BA graphs. Scale-free tend to be robust to errors, but sensitive to attacks.

In [22] is obtained the network that optimizes robustness for the sum of critical threshold for random deletion [9] and for deletion of central nodes [10].

Measures of network robustness: algebraic connectivity [17], effective graph resistance [16] and mutiscale vulnerability [6].

3 Cascading failures

In [21] is defined a first model of cascading failures. Load of a node is equal to number of shortest paths passing through it. Nodes with load above capacity are removed from the network. Evolution is tracked through size of connected component.

In the model of [11] load is also equal to number of shortest paths passing through it. They define a mechanism of load redistribution, and track evolution of damage through efficiency.

References

[1] Réka Albert, Hawoong Jeong, and Albert-László Barabási. Error and attack tolerance of complex networks. *Nature*, 406(6794):378–382, jul 2000.

> Complex networks are divided in two major classes. Exponential networks, with a degree distribution that peaks around average and decays exponentially. These networks are homogeneous, and high-degree nodes are statistically non-significant. Theoretical models of exponential networks are the Erdös-Rényi (ER) or Watts-Strogatz (WS) models. Scale-free networks have a degree distribution that decays with a power-law. These networks are non-homogeneous and high-degree nodes are statistically significant. These networks have a different behaviour facing errors (removal of nodes at random) and attacks (removal of nodes of high degree). ER networks are fragmented when a fraction f_c of nodes is reached when exposed to errors and attacks. Scale-free networks are very resilient to errors, but vulnerable to attacks. When attacked, scale-free networks are fragmented with a fraction of removed nodes smaller than the f_c of random graphs.

[2] Luís a Nunes Amaral, A Scala, M. Barthelemy, and H E Stanley. Classes of small-world networks. *Proceedings of the National Academy of Sciences*, 97(21):11149–11152, oct 2000.

> After empirical examination of real-world networks, authors identify three structural classes of small-world networks: a) scale-free networks, with a degree distribution with a tail that decays as a power law, b) broad-scale or truncated scale-free, with a degree distribution that has a power-law regime followed by a cutoff, like an exponential or Gaussian decay, c) single-scale networks, with a degree distribution with a fast-decaying tail, like exponential or Gaussian. The last two regimes can be reached modifying the preferential attachment mechanism introducing aging of vertices or introducing cost of adding links and limited capacity of highly connected nodes.

[3] J. Ash and D. Newth. Optimizing complex networks for resilience against cascading failure. *Physica A: Statistical Mechanics and its Applications*, 380(1-2):673–683, jul 2007.

> As authors adopt the Crucitti model of cascading failures to justify that maximizing network efficiency leads to reduction of cascading failures. Efficiency is optimized with two constraints: that the network have a single connected component, and that network connectivity (number of edges) is below a critical level. Optimization is made using a local search method with three moves: creating edges at random, deleting edges at random and rewiring existing connections. The resulting optimized network is of broad scale, and with a characteristic path length larger than scale-free networks.

[4] Albert-Laszlo Barabasi and Reka Albert. Emergence of scaling in random networks. *Science*, 286(5439):509–512, oct 1999.

Networks that grow through simultaneous growth and preferential attachment have a degree distribution decaying following a power law $k^{-\lambda}$ with $\lambda = 3$. Exponents of different value may appear caused by additional mechanisms, like connection of old nodes or existence of directed connections. As the same degree distribution is observed with different evolutions of size / time, this type of networks are known as scale-free.

[5] Albert-László Barabási, Réka Albert, and Hawoong Jeong. Scale-free characteristics of random networks: the topology of the world-wide web. *Physica A: Statistical Mechanics and its Applications*, 281(1-4):69–77, jun 2000.

The Barabasi-Albert model of scale-free networks is applied to the www network. According to this model, the mechanisms of growth and preferential attachment lead to a network with a degree distribution following a power law. This mechanism does not describe the www faithfully, but according to authors captures the main ingredients that structure the www. The actual structure of the www may depend of other characteristics, like nonlinear preferential attachment, rewiring of existing links or the appearance of new links.

[6] Stefano Boccaletti, Javier Buldú, Regino Criado, Julio Flores, Vito Latora, Javier Pello, and Miguel Romance. Multiscale vulnerability of complex networks. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 17(4):043110, dec 2007.

To analyze the impact of the deletion of one of several edges (without deleting any node) on graph connectivity, authors propose multiscale measures equal to the average edge betweenness. Graphs with an unequal distribution of loads will have higher values of edge betweenness and then will be more vulnerable. As the average betweenness is proportional to average path length, a complete exam of the scales $p > 0$ must be considered. In some cases might happen that two graphs may have equal values of vulnerability for $p = 1$ and $p = \infty$, so all scales must be considered. The formula for $p = -1$ yields a parameter similar to efficiency, but with edge betweenness instead of distances.

[7] Anna D. Broido and Aaron Clauset. Scale-free networks are rare. pages 26–28, 2018.

A central claim of modern network science is that real-world networks are typically scale-free, meaning that degree distribution follows a power law k^{γ} with $2 < \gamma < 3$. Authors test this claim with 927 data sets from the Index of Complex Networks (ICON), comparing its plausibility via a likelihood test to alternative models, e.g., log-normal. Results show that only a few fraction of these networks show strong evidence of being scale-free. Authors claim that there is likely no single universal mechanism (e.g., preferential attachment) that can explain the wide diversity of degree structure found in real-world networks.

[8] Ramon Ferrer i Cancho and Ricard V. Solé. Optimization in Complex Networks. pages 114–126. 2003.

Complex networks can be the outcome of preferential mechanisms and optimization mechanisms, plus additional constraints imposed by the available components to the evolving network. Optimization of networks is examined in this paper, where a energy objective function, combination of normalized vertex-vertex distance and normalized number of links. When normalized number of links has more weight, the resulting network has an exponential degree distribution, and when normalized vertex-vertex distance is predominant, the optimized network is a star network. For intermediate weights, the result of optimization is truncated scale-free networks.

[9] Reuven Cohen, Keren Erez, Daniel Ben-Avraham, and Shlomo Havlin. Resilience of the Internet to Random Breakdowns. *Physical Review Letters*, 85(21):4626–4628, nov 2000.

The article uses infinite percolation theory to obtain the critical threshold for networks with nodes connected randomly (not necessarily random networks). This threshold is the fraction of removed nodes at random that disconnects the network. For networks with a scale-free degree distribution k^γ, it is found that for $\gamma < 3$ the threshold diverges, so that the network keeps connected even for an arbitrarily large fraction of removed nodes.

[10] Reuven Cohen, Keren Erez, Daniel Ben-Avraham, and Shlomo Havlin. Breakdown of the Internet under Intentional Attack. *Physical Review Letters*, 86(16):3682–3685, apr 2001.

This article uses infinite percolation theory to analyze the effect of the removal of nodes of highest degree in scale free networks, with degree distribution k^γ. Results show that these networks are disrupted with the removal of a small fraction of nodes of highest connectivity for all $\gamma > 2$. Network robustness increases as lower connectivity cutoff m (smallest nonzero degree) increases. It is also observed that average path length in the spanning cluster grows dramatically near criticality, making communication very inefficient even before disruption of the spanning cluster.

[11] Paolo Crucitti, Vito Latora, and Massimo Marchiori. Model for cascading failures in complex networks. *Physical Review E*, 69(4):045104, apr 2004.

The dysfunction of a few nodes in a network transporting flows can initiate a dynamic process of cascading failures, as other nodes may experience malfunction if their load exceeds their capacity. In this model of cascading failures, overloaded nodes are not removed from the network, and the damage caused by a cascade is quantified in terms of decrease of global efficiency. In this model, the load of a node is proportional to the total number of most efficient paths passing through it, and capacity is proportional to its initial load and a tolerance parameter α for the network. In each iteration, the removal of a node changes the most efficient path between nodes and consequently the distribution of loads. Two triggering strategies are examined: random removals and load-based removals. ER and BA graphs react similarly to random removals, while BA graphs are more sensitive to load-based removals.

[12] Paolo Crucitti, Vito Latora, Massimo Marchiori, and Andrea Rapisarda. Efficiency of scale-free networks: error and attack tolerance. *Physica A: Statistical Mechanics and its Applications*, 320:622–642, mar 2003.

This paper reports the evolution of global (average path length and global efficiency) and local (clustering coefficient and local efficiency) properties of two models of scale-free networks when suffering errors (removal of random nodes) and attacks (removal of nodes of highest degree). The scale-free networks analyzed are the BA model, with low clustering coefficient, and the KE model, with high clustering coefficient. For these networks, global and local efficiencies are unaffected by the failure of random nodes, but extremely sensitive to the removal of high degree nodes. This paper defines the efficiency approach to static robustness in more detail than works from the same authors.

[13] Paolo Crucitti, Vito Latora, Massimo Marchiori, and Andrea Rapisarda. Error and attack tolerance of complex networks. *Physica A: Statistical Mechanics and its Applications*, 340(1-3):388–394, sep 2004.

The tolerance to errors (removal of random nodes) and attacks (removal of central nodes) on ER random networks and BA scale-free networks can be compared examining the impact on global efficiency of the removal of nodes chosen according to the following criteria: random, degree, betweenness and adaptive betweenness. As ER are homogeneous networks, they react similarly to all criteria, while BA networks are resilient to errors but vulnerable to attacks. The paper is complemented with the cascading failures model based on load redistribution.

[14] Liang Dai, Ben Derudder, and Xingjian Liu. The evolving structure of the Southeast Asian air transport network through the lens of complex networks, 1979–2012. *Journal of Transport Geography*, 68(October 2017):67–77, apr 2018.

The article explores the structural evolution of the Southeast Asian air transport network (SAAN) during 1979-2004 from a complex network perspective. First, authors study the evolution of network metrics (scale-free properties, dissortative mixing and small-world properties), and compare them with other major regional blocs. Second, they unveil the core-bridge-periphery structure of the SANN, and its temporal evolution. This multilayer structure has experienced significant changes in the studied period, as the core of the network shifts towards the north. Additionnally, the introduction contains an geographical and historical analysis of Southeast Asia, and discuss the opportunity of defining region boundarys to analyze transportation networks.

[15] Kousik Das, Sovan Samanta, and Madhumangal Pal. Study on centrality measures in social networks: a survey. *Social Network Analysis and Mining*, 8(1):13, dec 2018.

An article with awful writing and structuring. Can be of interest to check some centralities for characterizing important nodes, not necessarily on complex networks, like the ones based on k-core decomposition (k-shell centrality) or in number of closed loops (subgraph centrality and functional centrality).

[16] W. Ellens, F.M. Spieksma, P. Van Mieghem, A. Jamakovic, and R.E. Kooij. Effective graph resistance. *Linear Algebra and its Applications*, 435(10):2491–2506, nov 2011.

In this context, a graph is treated as a electrical circuit, with resistance between vertices equal to edge weights. The effective resistance between two vertices is obtained applying Kirchhoff laws when a difference of potential is applied between these nodes, and effective graph resistance is equal to the sum of the effective resistances over all pair of vertices. Effective resistance is infinite for non-connected graphs, and will decrease as graph connectivity increases by adding edges or increasing edge weights. It can be used as a measure of robustness as takes the number of paths between any pair of vertices and their length into account. It can be calculated as the sum of reciprocals of the eigenvalues of the Laplacian, excluding the smallest eigenvalue. The paper provides computation procedures and defines graphs of optimal effective resistance.

[17] Miroslav Fiedler. Algebraic connectivity of graphs. *Czechoslovak Mathematical Journal*, 23(2398):298–305, 1973.

The algebraic connectivity of a graph is the second smallest eigenvalue of the Laplacian of a graph. Diagonal of the Laplacian is equal to node degree, and the off diagonal elements equal to -1 if edge (i, j) exists and zero otherwise. In this paper is denoted as $a(G)$, and as λ_2 elsewhere. It is related with two other concepts: edge connectivity $e(G)$, or the minimal number of edges whose removal results in losing connectivity, and vertex connectivity $v(G)$ is defined similarly for removal of vertices together with adjacent edges. Algebraic connectivity is greater than zero if and only if G is a connected graph. The magnitude of this value reflects how well connected the overall graph is, so that the larger is, the better connected the graph is. For non-complete graphs, $a(G) \leq v(G)$, and $v(G) \leq e(G)$.

[18] Konstantin Klemm and Víctor M. Eguíluz. Growing scale-free networks with small-world behavior. *Physical Review E*, 65(5):057102, may 2002.

This is an attempt to explain the dynamic behaviour of complex networks by a model of network self-organization that creates networks with a degree distribution with a power law decay and the small world property. This model adds a node in each iteration with the following rules. The graph start with a complete graph of m active nodes, and in each iteration a new node is included following three steps. 1) the new node has m links. Each link is attaching the new node to an active node with probability $1-\mu$ or to any node according with linear preferential attachment with probability μ. 2) The new node becomes active, 3) One of the active nodes is deactivated with a probability proportional to the reciprocal of the degree. With $\mu = 0$ we obtain the BA model, and with $\mu \gg 1$ a scale-free graph with the small-world property.

[19] Gueorgi Kossinets and Duncan J Watts. Empirical analysis of an evolving social network. *Science*, 311(5757):88–90, jan 2006.

Authors analyze a social network of e-mail interactions in a population of 43,553 members of a university, retaining 14,584,423 messages exchanged during 355 days of observation. They approximate instantaneous strength of a relationship by the geometric rate of bilateral email exchange within a window of 60 days. The instantaneous network at any point of time includes all pairs of individuals that sent one of more messages in each direction in the last 60 days. Using the later representation, they calculate the shortest path length and the number of shared affiliations for all members during 210 days. Appearance of new ties is assessed with two measures. Cyclic closure bias is the empirical probability that two individuals initiate a new tie as a function of shortest path length. Focal closure bias is the probability that two individuals who share an interaction focus share a new tie. For this network, average network properties appear to approach an equilibrium state, while individual properties are unstable.

[20] Vito Latora and Massimo Marchiori. Efficient Behavior of Small-World Networks. *Physical Review Letters*, 87(19):198701, oct 2001.

The small world property and complex networks can be expressed in terms of global and local efficiency, two measures of how efficiently information is exchanged over the network. As communication between nodes will take place along the shortest paths connecting them, efficiency of communication is defined as inversely proportional to shortest distance $\epsilon_{ij} = 1/d_{ij}$. Global efficiency E_{glob} is equal to the average value of ϵ_{ij}, and local efficiency E_{loc} to the average value of the efficiency of the local subgraphs of each node. Both measures are normalized, taking values between zero and one. As $1/L$ and C are first approximations of E_{glob} and E_{loc}, small-world graphs have high values of E_{glob} and E_{loc}, and therefore are efficient in transporting information globally and locally. Global and local efficiency are defined for weighted and/or unconnected graphs.

[21] Adilson E. Motter and Ying-Cheng Lai. Cascade-based attacks on complex networks. *Physical Review E*, 66(6):065102, dec 2002.

Authors introduce a model for cascading failures in complex networks, suitable for networks that vehiculate flows of information, energy of physical quantities. In these networks, the load of a node is equal to the total number of shortest paths passing through it (sometimes approximated by node betweenness). The capacity of a node is proportional to its initial load. The failure of a node can lead to a redistribution of loads, that can conversely lead to the failure of nodes in which capacity is exceeded. Authors find that cascading failures occur in networks with a highly heterogeneous distribution of loads (e.g., scale-free networks), when the removed nodes are among those of higher load.

[22] G. Paul, T. Tanizawa, S. Havlin, and H. E. Stanley. Optimization of robustness of complex networks. *The European Physical Journal B*, 48(1):149–149, nov 2005.

The goal of this research is to maximize the robustness of a network of N nodes to random failures and targeted attacks with the constraint that the cost remains constant. Cost is supposed proportional to the number of edges. Robustness is measured as the sum of thresholds for random and targeted removal of nodes. The resulting network has a degree distribution with only two values, obtained connecting $k_2 \sim AN^{2/3}$ nodes to a single node. The rest of nodes are of degree k_1.

[23] Shuliang Wang, Liu Hong, Min Ouyang, Jianhua Zhang, and Xueguang Chen. Vulnerability analysis of interdependent infrastructure systems under edge attack strategies. *Safety Science*, 51(1):328–337, jan 2013.

This paper analyzes the vulnerability of a two interdependent networked systems to cascading failures: a power grid and a gas network. The cascading failure model of the power grid is the defined in Wang et al. (2008), where edge load is proportional to the power of product of edge's nodes. The model for the gas network is the generalized betweenness centrality model defined in Carvalho et al. (2009). Network interdependence is modeled through a specific interdependence function. Nodes that lead to interdependence are detected using spatial proximity criteria. Authors define three categories of network disturbance: random failures, deliberate attacks and natural disasters. Deliberate attacks are defined as suppression of edges of high load and nodes of high degree. The results of the vulnerability metrics are global vulnerability analysis and critical component analysis. Global vulnerability is measured with network efficiency and damaging rate. Critical component analysis reports the network components whose damage would lead to larger vulnerability.

[24] Duncan J Watts and Steven H Strogatz. Collective dynamics of 'small-world' networks. *Nature*, 393(6684):440–2, jun 1998.

Small-world networks can be obtain starting with a ring lattice with n nodes and k edges per node, and rewiring each edge at random with probability p. With $p = 0$ we have a regular high-clustered lattice whose characteristic path length L grows linearly with n, and with $p = 1$ a poorly-clustered random graph where L grows logarithmically with n. There is a broad range of values of p where L is similar to L_{random} and $C \gg C_{random}$, being C the average clustering coefficient. The small-world property, defined as the coexistence of a low L with a high C is present in a large number of real-world networks.