Annotated bibliography on complex networks

Jose M Sallan

1 Static robustness

In [10] is obtained the network that optimizes robustness for the sum of critical threshold for random deletion [4] and for deletion of central nodes [5].

References

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

To be annotated.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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).

[8] 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.

[9] 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.

[10] 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.

[11] 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.