# 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 [44] 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 [31] 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 [28] is defined a KE generative model of highly-clustered scale-free networks. In Refs. [22] and [40] can be found other network models with power-law degree distribution, short average path length and high clustering coefficient.

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 [9].

## 2 Air transport networks

[32] makes a complex network and spatial analysis of the Chinese air transport network.

[47] is a review of studies of air transport networks. The section of dynamic models of air transport is of special interest, especially for the referenced studies of connectivity [8] and [34].

## 3 Static robustness

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

Analysis of static robustness in terms of network efficiency: [13] for BA and KE graphs, [14] for BA graphs. Scale-free tend to be robust to errors, but sensitive to attacks. In Ref. [24] is performed an analysis of the effect of edge and node removal for several real-world and models of complex networks.

In [39] is obtained the network that optimizes robustness for the sum of critical threshold for random deletion [10] and for deletion of central nodes [11].

Measures of network robustness: algebraic connectivity [20], effective graph resistance [18] and mutiscale vulnerability [6].

Schneider and colleagues [41] define a unique network robustness measure (in [25] is described a procedure to compute an approximate value). They optimize this measure rewiring network nodes, maintaining the degree of each node. Refinements of this strategy can be found in [33, 45, 48].

# 4 Cascading failures

In Ref. [38] is defined a global load-based model of cascading failures. Node load 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 Ref. [12] is defined an similar model, and track evolution of damage through network efficiency.

In Ref. [43] is defined a local weighted flow redistribution rule model for cascading failures. In this model, the load of congested edges is redistributed locally, among the adjacent edges.

In Ref. [36] is defined a fiber-bundle model of cascading failures, and in [26] a sandpile model for a geographical network.

Holme and colleagues analyze the cascading failures for node [23] and edge [21] overload in growing networks. As the network grows, values of node or edge betweenness increase, so when they reach a critical point a cascading failure may arise.

# 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 $k^\gamma$ 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] Guillaume Burghouwt and Jaap de Wit. Temporal configurations of European airline networks. *Journal of Air Transport Management*, 11(3):185–198, may 2005.

Spatial and temporal concentration are the two main features of the hub-and-spoke network. Airlines using an hub-and-spoke configuration organize their flights in a wave-system structure, that helps them to offer many indirect connections around a hub. In this paper, authors define a methodology to detect wave-system structures, and define a metric of indirect connectivity based on the number and quality of indirect connections generated by a flight schedule. The later metric is based on previous work reporting passengers' preferences with indirect connections. They use these concepts to analyze the effects of a wave-system structure on indirect connectivity.

[9] 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.

[10] 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 $k^{\gamma}$, 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.

[11] 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 $k^{\gamma}$. 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.

[12] 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 $\alpha$ for the network. The overload of a node degrades the communication through edges incident to that node, so shortest paths will go through other nodes. 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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).

[17] Bing-Lin Dou, Xue-Guang Wang, and Shi-Yong Zhang. Robustness of networks against cascading failures. *Physica A: Statistical Mechanics and its Applications*, 389(11):2310–2317, jun 2010.

> This paper proposes a modification of the Motter and Lai (ML) model of cascading failures. The ML model proposes that node capacity is proportional to initial load $C_i = (1+\alpha)\,L_{0i}$, and here authors suggest a load equal to $C_i = L_{0i} + \beta L_{0i}^{\alpha}$. This model is applied to BA and ER networks and to the power grid and the internet. The contribution is rather limited, as the justification for a nonlinear load is weak.

[18] 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.

[19] Klaus Fiedler. Tools, Toys, Truisms, and Theories: Some Thoughts on the Creative Cycle of Theory Formation. *Personality and Social Psychology Review*, 8(2):123–131, may 2004.

This article studies the creative process of theory formation, and how theoretical thinking can be instigated and trained. Drawing on Moscovici's approach to social influence of majorities and minorities, author sees theory formation as a dialectic interplay between conversion (break-up with existing theories by the minorities) and compliance (establishment of existing theories by the majority). Author also argues that theoretical thinking can be instigated and trained with game-like heuristics. Loosening games are pluralistic-competition, distal-import and paying around with tools and methods. Tightening games are falsification and challenge (as in peer review), method-development and uncovering of pseudo-theories (quasi tautological theoretical constructions).

[20] 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 $\lambda_2$ 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 $v(G) \leq e(G)$.

[21] Petter Holme. Edge overload breakdown in evolving networks. *Physical Review E*, 66(3):036119, sep 2002.

This paper analyzes the possibility of breakdown of an evolving network by overload of edges. Load is equal to edge betweenness computed for a number of paths proportional to $N(N-1)$. Capacity is constant and equal for all edges. As the network grows, the load of edges may increase beyond capacity, triggering a cascading failure process. Two evolving networks are examined: the original BA model with preferential attachment, and a variant of the BA with random attachment. The effects of edge overload have a lesser impact than node overload, studied in [23].

[22] Petter Holme and Beom Jun Kim. Growing scale-free networks with tunable clustering. *Physical Review E*, 65(2):026107, jan 2002.

This work proposes a network model which has both the perfect power-law degree distribution and the high clustering. Clustering coefficient is tunable by adjusting a parameter in the model. Clustering is added via a triad formation (TF) mechanism, which can be triggered after a preferential attachment (PA) with a probability $P_t$: If an edge between $v$ and $w$ was added in the previous PA step, then add one more edge from $v$ to a randomly chosen neighbor of $w$. If there remains no pair to connect, i.e., if all neighbors of w were already connected to v, do a PA step instead. The clustering is tuned by fixing the parameter $P_t$.

[23] Petter Holme and Beom Jun Kim. Vertex overload breakdown in evolving networks. *Physical Review E*, 65(6):066109, jun 2002.

This paper analyzes the possibility of breakdown of an evolving network by overload of nodes. Load is equal to node betweenness computed for a number of paths proportional to $(N-1)\,(N-2)$ for the extrinsic communication activity (ECA) case, and to $(N-1)$ for the intrinsic communication activity (ICA) case. Capacity is equal for all nodes. For the ICA case, is constant and for ICA grows linearly with $N$. As the network grows, the load of nodes may increase beyond capacity, triggering a cascading failure process. Two evolving networks are examined: the original BA model with preferential attachment, and a variant of the BA with random attachment. Interestingly, preferential attachment increases the probability of a giant component to form compared to random connection. In Ref. [21] can be found a similar study with edge overload.

[24] Petter Holme, Beom Jun Kim, Chang No Yoon, and Seung Kee Han. Attack vulnerability of complex networks. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 55(1):65–69, feb 2002.

This study measures attack vulnerability of various complex network models and real world networks. The attack strategies considered are removal of vertices and edges by initial degree (ID), initial betweenness (IB), recalculated degree (RD) and recalculated betweenness (RB). The measure of edge degree considered is the product of the degree of vertices connected by the edge. As network performance measures, authors consider the size of giant component and the average inverse geodesic length (ldesigned as network efficiency in [31]. The real world networks considered are the scientific collaboration network and a computer network for Internet traffic. The theoretical models considered are ER, WS, BA and a clustered scale-free network model (CSF). Results shows that none of the network models shows a behaviour very similar to real world networks, suggesting that there are other structures contributing to network behaviour. The

ER model, which lacks structural bias, is the most robust of the tested networks.

[25] Chen Hong, Ning He, Oriol Lordan, Bo-Yuan Liang, and Nai-Yu Yin. Efficient calculation of the robustness measure R for complex networks. *Physica A: Statistical Mechanics and its Applications*, 478:63–68, jul 2017.

The calculation of the Schneider's unique robustness measure $R$ can be very costly, as the size of the largest connected component has to be assessed $N$ times. In this article an aproximation of $R$ is suggested consisting in stopping the calculation once the largest connected component is below a given value.

[26] Liang Huang, Lei Yang, and Kongqing Yang. Geographical effects on cascading breakdowns of scale-free networks. *Physical Review E*, 73(3):036102, mar 2006.

To be reviewed later

[27] Ehsan Jahanpour and Xin Chen. Analysis of complex network performance and heuristic node removal strategies. *Communications in Nonlinear Science and Numerical Simulation*, 18(12):3458–3468, dec 2013.

The paper analyzes the performance of node removal strategies on the Krebs network of relationships between hijackers that participated on the September 11, 2001 attacks. The strategies are one-time (non-adaptive) and multiple-time (adaptive) based on degree, betweenness, reciprocal closeness, complement-derived closeness and eigenvector, and additionally random removal of nodes. Network performance measures are focused on diffusion speed measures (network reciprocal distance and average node coverage), diffusion scale (largest coverage probability and expected scale) and structural properties (shortest distance homogeneity and network diameter). This work neglects most of previous developments (e.g., network reciprocal distance is quite similar to network efficiency, and impact of network topology on robustness is not discussed), and the analysis is carried out in a single, small network.

[28] 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 $\mu$. 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.

[29] Yakup Koç, Martijn Warnier, Robert E. Kooij, and Frances M.T. Brazier. An entropy-based metric to quantify the robustness of power grids against cascading failures. *Safety Science*, 59:126–134, nov 2013.

> This paper proposes a metric that quantifies robustness of a power transmission grid with respect to cascading failures by targeted attacks. The measure is defined specifically for power grids, and takes into account network structure and the operative state of the network. The metric is the product of electrical nodal robustness and electrical node significance. Electrical nodal robustness is based on entropy, to take into account load heterogeneity and out-degree of each node. Electrical node significance is the power distributed by each node, normalized by the sum of values for each node. This measure captures the robustness of power grids to targeted attacks of edges, measured empirically by demand, link and capacity survivability.

[30] 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.

[31] 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 $\epsilon_{ij}$, 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.

[32] Jingyi Lin. Network analysis of China's aviation system, statistical and spatial structure. *Journal of Transport Geography*, 22:109–117, may 2012.

This paper reports the analysis of the Chinese air transportation network. The study includes analysis of small-world and scale-free properties, distribution of node degree and strength (with edge weights equal to number of flights), correlational analysis (the network has dissortative mixing) and hierarchical structure. Hierarchical structure is measured through correlation of degree and strength with clustering coefficient. Contrary to theoretical expectations for distance-driven networks, the analyzed aviation network presents hierarchical structure. Finally, authors conduct a spatial analysis studying frequency of distances and flows versus distances, and use gravitational models to analyze distance decay in terms of weight, population and GDP. Results show that traffic between cities is proportional to product of centrality and inversely proportional to distance.

[33] V. H. P. Louzada, F. Daolio, H. J. Herrmann, and M. Tomassini. Smart rewiring for network robustness. *Journal of Complex Networks*, 1(2):150–159, dec 2013.

This article proposes an improvement of the mitigation method of [41] for increasing network robustness. In this method, five nodes previously connected are transformed into a triangle and a pair of nodes. This method increases robustness by adding links between nodes of average degree. They also define a onionlikeness parameter to evaluate the degree to which a network has a onion structure, associated with high values of robustness. They find that after the smart rewiring process, network modularity and assortativity increases, so the resulting network has a *modular onion* structure.

[34] Paolo Malighetti, Stefano Paleari, and Renato Redondi. Connectivity of the European airport network: "Self-help hubbing" and business implications. *Journal of Air Transport Management*, 14(2):53–65, mar 2008.

Most of the potential of indirect connectivity of air transport networks is exploited by alliance systems, but there may be also potential for additional connectivity from "self-hubbing" connections established by users of low-cost and conventional airlines. This paper explores these possibilities of connection finding the paths of minimum travel time for a time window, or for a specific time of a time window. Based on these shortest paths, they can compute the betweenness and essential betweenness of each airport, which is a metric of indirect connectivity, and study in detail airport connectivity. Authors analyze the European air transport network for a time window of 24 hours.

[35] Igor Mishkovski, Mario Biey, and Ljupco Kocarev. Vulnerability of complex networks. *Communications in Nonlinear Science and Numerical Simulation*, 16(1):341–349, jan 2011.

Drawing on previous research by [6] the value of average edge betweenness is considered as a measure of vulnerability: the lower the average edge betweenness, the less vulnerable the network is. To this value, authors add two more values: the change of average edge betweenness when some important nodes or edges have been removed, respectively, to create a vulnerability index. It is unclear (or undefined) the number of nodes or edges to be removed, and how vulnerability indices can be compared.

[36] Y. Moreno, J. B. Gómez, and A. F. Pacheco. Instability of scale-free networks under node-breaking avalanches. *Europhysics Letters*, 58(4):630–636, 2002.

This article defines a fiber bundle model for cascading failures in complex networks. Each node has a security threshold, usually following a Weibull distribution. In the starting point, the networks is exposed to a external force $F$, so each node bears a load of $\sigma = F/N$. All nodes with a load higher than their threshold are disconnected, and then the load of the disconnected nodes is equally transferred to the non-failed nodes directly linked to it, which in turn may lead to these nodes to collapse. The process ends where there are no new collapsed nodes. This process is tested in a BA network. The cascading process has a critical point. This critical point is larger, and more abrupt, for more homogeneous Weibull distributions, and smaller for uniform distributions.

[37] Y. Moreno, R. Pastor-Satorras, A Vázquez, and A. Vespignani. Critical load and congestion instabilities in scale-free networks. *Europhysics Letters (EPL)*, 62(2):292–298, apr 2003.

The appearance of cascading failures in communication networks is analyzed here with a threshold model, where each link has a load coming from a random distribution with mean equal to average load $\langle \updownarrow \rangle$. Capacity of all links is set equal to one. Load of congested nodes is redistributed following two alternative rules: equally among neighbour nodes or randomly. If a link is congested and has no neighbours, the load can be assigned equally to other links (non-dissipative model) or considered lost (dissipative model). When this model is applied to scale-free networks, there is a range of values of $\langle \updownarrow \rangle$ where there is a small but relevant probability that the system collapses. This can explain why communication networks like the Internet can suffer cascading failures as load increases.

[38] 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.

[39] 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 $k_1$.

[40] Erzsébet Ravasz and Albert-László Barabási. Hierarchical organization in complex networks. *Physical Review E*, 67(2):026112, feb 2003.

The scale-free topology and the high average clustering present in many real-world networks can be modelled through a hierarchical network. In this network, degree distribution follows a power law with exponent $\gamma$, and clustering coefficient is related with node degree with a scaling law of exponent $\beta$. These networks are modular, in the sense that they have many small, densely interconnected clusters, that combine recursively forming larger, but less cohesive groups. The hubs, nodes with high degree and low clustering coefficient, bridge the many small communities into a single, integrated network. The examination of real-world networks shows evidence of hierarchical organization in many real-world networks (the actor and language networks), but not in networks with a geographic organization (the Internet at the autonomous system level or the power grid). The clustering coefficient of the later is independent of node degree.

[41] Christian M. Schneider, Andre A. Moreira, Jose S. Andrade, Shlomo Havlin, and Hans J. Herrmann. Mitigation of malicious attacks on networks. *Proceedings of the National Academy of Sciences*, 108(10):3838–3841, mar 2011.

Authors describe a mitigation method to increase network robustness that keeps invariant the total number of links and the degree of each node. They also define a unique robustness measure $R$ that assesses the evolution of the size of the largest connected cluster as a function of the fraction of removed nodes. The method consists in selecting two edges at random $e_{ij}$ and $e_{kl}$, and replace them by $e_{ik}$ and $e_j$ if this change increases $R$. Depending on the type of network, additional constraints can be added. A small fraction of edge changes increases robustness significantly. The resulting networks have a onion-like structure, consisting of a core of highly connected nodes hierarchically surrounded by rings of nodes of decreasing degree.

[42] 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.

[43] Wen-Xu Wang and Guanrong Chen. Universal robustness characteristic of weighted networks against cascading failure. *Physical Review E*, 77(2):026101, feb 2008.

The paper describes a local weighted flow redistribution rule (LWFRL) to model cascading failures. Each edge has a weight equal to $(k_i k_j)^\theta$, and a capacity proportional to its initial weight. Every time an edge is overloaded, its weight is redistributed among edges attached to node edges $i$ and $j$. The rule is tested in Barabási-Albert (BA) and Newman-Watts (NW) models, finding that maximum robustness is achieved for $\theta = 1$. This result is attained via computational experiments and analytic development.

[44] 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.

[45] Yang Yang, Zhoujun Li, Yan Chen, Xiaoming Zhang, and Senzhang Wang. Improving the Robustness of Complex Networks with Preserving Community Structure. *PLOS ONE*, 10(2):e0116551, feb 2015.

This paper presents a method for increasing network robustness preserving the community structure. The method has three steps: first, make each community tend to a onion-like structure; second, swap edges to make vertices with high importance (node degree) only connect with vertices of the same community; third, swap edges to increase the number of edges among communities. To design robust networks with community structure, authors suggest that each community is designed as an onion-like structure, and connect communities with edges between vertices of low degree. They also advance that structural diversity (the number of each possible 3-node and 4-node subgraphs) can play a role in network robustness, and that the best strategies to attack networks can be different for networks with strong and weak community structure.

[46] Massimiliano Zanin, Lucas Lacasa, and Miguel Cea. Dynamics in scheduled networks. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 19(2):023111, jun 2009.

To take into account the fact that air connections are planned with scheduled flights, here is presented a scheduled network formalism. This formalism defines an adjacency matrix including a differential adjacency matrix which is constant and represents one time step, and an activation matrix holding the scheduling information. Authors deduce network properties and metrics of tolerance of errors and attacks from this formalism.

[47] Massimiliano Zanin and Fabrizio Lillo. Modelling the air transport with complex networks: A short review. *The European Physical Journal Special Topics*, 215(1):5–21, jan 2013.

This review covers the state of the art of analysis of air transport networks through complex network analysis in 2010. The most common representation of air transport networks is called here flight networks: nodes as airports connected with unweighted, undirected links if there is at least a direct flight between them. The review covers the following topics: network definition, topological analysis, dynamics on the air network (including indirect connectivity, air traffic jams and epidemic spreading) and resilience and vulnerability (very short, missing some contributions).

[48] Mingxing Zhou and Jing Liu. A memetic algorithm for enhancing the robustness of scale-free networks against malicious attacks. *Physica A: Statistical Mechanics and its Applications*, 410:131–143, sep 2014.

Networks with high robustness have a onion-like structure, where nodes of the same degree are connected. Here a memetic algorithm is defined to create this structure, optimizing Schneider's unique robustness measure $R$. This memetic algorithm requires the definition of a crossover operator, and of a local search operator. In the later, a node swap is accepted if nodes are connected to others of similar degree. The bibliography includes other examples of metaheuristics to improve network robustness.