6

Resilience and robustness of networks

The large-scale collapses of the electric distribution grid or internet outages have shown that the stability of complex networks is a problem of crucial importance. The protection of critical infrastructures or the elaboration of efficient reaction strategies all rely on the identification of crucial (or weak) elements of the network and on the understanding of the progressive damage caused by successive removals or failures of nodes. In this context, it has been observed that complex network models usually display great stability even if they are confronted by a large number of repeated small failures, while at the same time major damage can be triggered, unpredictably, by apparently small shocks. This is also consistent with empirical experience in which unexpected, small perturbations may sometimes trigger large systemic failures.

In this chapter, we deal with the impact of the removal or failure of nodes in complex networks by studying their percolation behavior. Percolation models and the associated critical phenomena have been extensively studied in statistical physics and, even though they are not endowed with a high level of realism, they can be thought of as the zeroth order approximation to a wide range of damaging processes. In particular we focus on heterogeneous networks that typically display both a large robustness to random failures and a high vulnerability to targeted attacks on the most crucial nodes. These two aspects elucidate how the topology of a network influences its stability and integrity, and highlight the role of hubs and connectivity fluctuations.

6.1 Damaging networks

The simplest assessment of networks' behavior in the case of progressive levels of damage can be obtained by studying the effect of removal of nodes on the network structure. While this approach focuses on the bare topological impact of damage and neglects all the issues related to the detailed technical aspects of the system's

https://doi.org/10.1017/CBO9780511791383.007 Published online by Cambridge University Press

elements and architecture, it provides an initial insight into the potential effects of failures in large-scale networks. In this spirit, Albert, Jeong and Barabási (2000) have made a comparative study of the topological effects of removal of nodes in various graph representations of real-world networked systems with either homogeneous or heterogeneous topologies. Albert *et al.* (2000) consider the damage created by removing a certain fraction of nodes or links, either in a random manner (to model a random failure), or in a "targeted" way to mimic intentional damage as illustrated in Figure 6.1. Targeted attacks are carried out by removing nodes preferentially according to their "centrality" (either measured by the degree or the betweenness centrality) and can describe intentional attacks supposed to maximize the damage by focusing on important hubs. The evidence put forward by Albert *et al.* (2000) is that heterogeneous and homogeneous topologies react very differently to increasing levels of damage.

In order to characterize the phenomenology associated to the damage process we need to define a quantitative measure of network damage. To this end, we consider a network in which a certain fraction f of the nodes has been removed and each time a node is removed, all links going from this node to other nodes of the network are deleted as well. Such damage may break an initially connected graph into

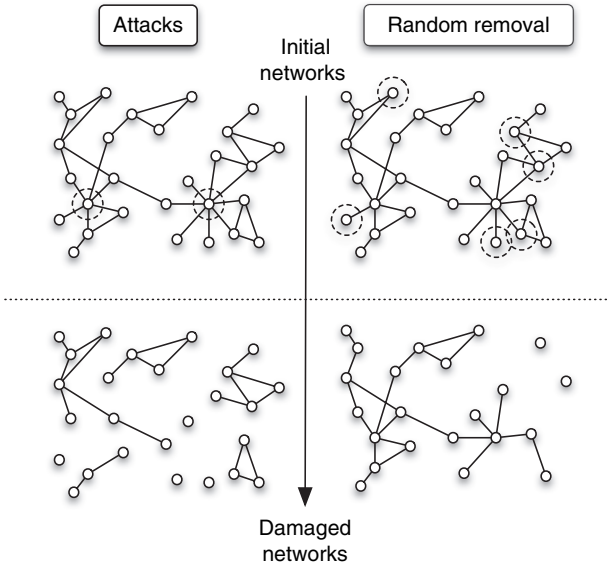

Fig. 6.1. Schematic comparison of random and targeted removal. On the left, we show the effects of targeted attacks on the two nodes with largest degrees. The resulting network is made of small disconnected components. In the case of random removal of six nodes (right column), the damage is much less significant as there is still a path between most of the nodes of the inital network.

https://doi.org/10.1017/CBO9780511791383.007 Published online by Cambridge University Press

various disconnected pieces. The simplest quantitative measure of damage is therefore given by the relative size of the largest connected component of the remaining network, S_f/S_0, where $S_0 = N$ is the original size of the network. The network will indeed keep its ability to perform its tasks as long as a "giant cluster" of size comparable to the original one (S_0) exists. When $S_f \ll S_0$, the network has been broken into many small disconnected parts and is no longer functional. The study of the evolution of S_f/S_0 as a function of the fraction of removed nodes f therefore characterizes the network response to damage, as shown in Figure 6.2 for both random and targeted removal of nodes. At low levels of damage, the resilience in the random removal process is essentially determined by local details, such as the minimum degree. At large levels of damage, homogeneous graphs exhibit a definite level of damage over which S_f/S_0 abruptly drops to zero, signaling the total fragmentation of the network. Heterogeneous networks on the contrary appear to lack a definite threshold and display higher tolerance to large random damage. It is possible to achieve a basic understanding of this evidence by recalling that the heavy-tailed form of the degree distribution of heterogeneous networks implies that the vast majority of vertices have a very small degree, while a few hubs collect a

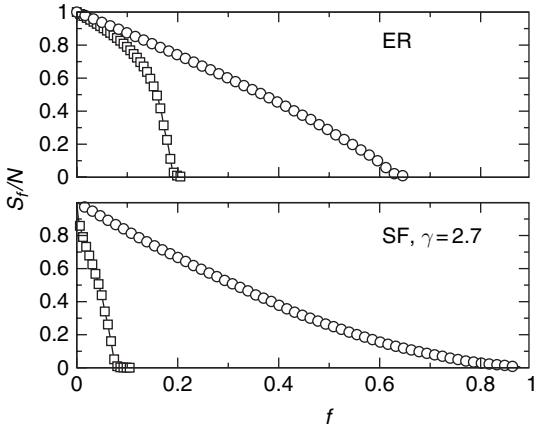

Fig. 6.2. Size S_f of the giant component (largest connected component) divided by the initial size $S_0 = N$ of the network, vs. the fraction f of removed nodes, for random removal (circles) or targeted attacks (squares). Two networks are considered: a homogeneous Erdős–Rényi (ER) network of $N = 10^5$ nodes and average degree $\langle k \rangle \sim 3$, and a generalized random scale-free (SF) network with same size, and average degree and distribution $P(k) \sim k^{-\gamma}$, $\gamma = 2.7$. In the heterogeneous (SF) network suffering random removals, the giant component decrease does not exhibit a definite threshold as in the case of the Erdős–Rényi network. The damage caused by targeted attacks, on the contrary, is much larger than in the case of the Erdős–Rényi network.

https://doi.org/10.1017/CBO9780511791383.007 Published online by Cambridge University Press

very large number of edges, providing the necessary connectivity to the whole network. When removing vertices at random, chances are that the largest fraction of deleted elements will have a very small degree. Their deletion will imply, in turn, that only a limited number of adjacent edges are eliminated. Therefore, the overall damage exerted on the network's global connectivity properties will be limited, even for very large values of f.

The picture is very different in the case of targeted attacks. The first vertex which is removed has the highest degree. Then the second highest degree vertex is removed, and so on until the total number of removed vertices represents a fraction f of the total number of vertices forming the original network. In Figure 6.2, the topological resilience to targeted attacks of heterogeneous graphs is compared with that of an Erdős–Rényi graph with the same average degree. In this case the emerging scenario appears in sharp contrast with the one found for the random removal damage. The heterogeneous graphs strikingly appear much more vulnerable than the Erdős–Rényi random graph. Obviously, they are more vulnerable than a regular lattice for which a degree-based targeted attack cannot be properly defined (all vertices have the same degree), which can thus be considered to have the same resilience as in the random removal case. In other words, in heavy-tailed networks, the removal of a small fraction of the largest degree nodes has a disproportionate effect that drastically reduces the size of the largest connected component of the network. The different behavior of heterogeneous and homogeneous networks is not unexpected and can be understood in terms of their degree distributions. The heavy-tailed nature of the heterogeneous networks makes the hubs extremely important to keep the graph connected. Their removal leads right away to network collapse. On the other hand, homogeneous graphs such as Erdős–Rényi graphs have exponentially decaying degree distributions in which the probability of finding a hub is exponentially small. Statistically, the vertices' degree is almost constant around their average values, and a targeted attack, while still performing better than a random removal, does not reach the extreme efficiency achieved in scale-free networks.

It is worth remarking that other possible quantitative measures of topological damage can be defined in networks. For example, the increase in the average path length between pairs of nodes indicates how communication becomes less efficient. When the removal of nodes leads to the disruption of the original network into disconnected clusters, the average shortest path length of the whole network in fact diverges (the distance between two non-connected nodes being infinite). An interesting way to avoid this problem consists in using the average inverse geodesic length (also called efficiency; Latora and Marchiori [2001]) defined as

$$\frac{1}{N(N-1)} \sum_{i \neq j} \frac{1}{\ell_{ij}}, \tag{6.1}$$

https://doi.org/10.1017/CBO9780511791383.007 Published online by Cambridge University Press

where ℓ_{ij} is the shortest path length between the nodes i and j. This quantity is finite even for disconnected graphs because each pair of disconnected nodes is assumed to have $\ell_{ij} = \infty$ and adds a null contribution to the efficiency expression. In weighted networks, other measures have to be defined in order to take into account that some nodes or links are more important than others: the integrity of a network is quantified by the largest sum of the weights in a connected component, giving the amount of connected traffic that the damaged network is still able to handle (see Section 6.5.2).

It is important to stress that different definitions of the damage do not change the general picture of the different behavior of heterogeneous and homogeneous networks under attack. In summary, while homogeneous networks suffer damage similarly in the different strategies, heterogeneous networks appear resistant to random failure and quite fragile with respect to targeted attacks. While not completely unexpected, the result is surprising in that the two kinds of damages do not just differ quantitatively but exhibit very distinct functional behavior in contrast to what happens in homogeneous networks. In particular, heterogeneous networks appear to lack a definite threshold in the case of random failures. This intuition and the handwaving considerations presented here find a solid theoretical ground in the analytical solution of percolation models on random graphs.

6.2 Percolation phenomena as critical phase transitions

Percolation theory provides the natural theoretical framework to understand the topological effect of removing nodes (Bunde and Havlin, 1991; Stauffer and Aharony, 1992). Simply stated, the percolation problem considers an arbitrary network topology in which each node is occupied with probability p and links are present only between occupied nodes. As the probability p increases, connected components – called clusters in this context – emerge. Such a set-up defines the site percolation problem that studies the properties of the clusters, and in particular their sizes, as a function of the occupation probability p. It is indeed intuitively clear that if p is small, only small clusters can be formed, while at large p the structure of the original network will be almost preserved (if $p = 1$ the network is completely recovered). In this context the removal of a fraction f of randomly selected nodes is just equivalent to considering that each site of the network is occupied with probability $p = 1 - f$.

For the sake of simplicity let us first consider a two-dimensional lattice such as the one depicted in Figure 6.3. At low occupation probability, only isolated nodes and small clusters of occupied sites are obtained. At large enough p, in contrast, one observes larger clusters and in particular a *percolating* cluster which spans the lattice by a connected path of occupied sites. Similarly, the *bond percolation* problem considers that the edges of the lattice can be either occupied or empty with

https://doi.org/10.1017/CBO9780511791383.007 Published online by Cambridge University Press

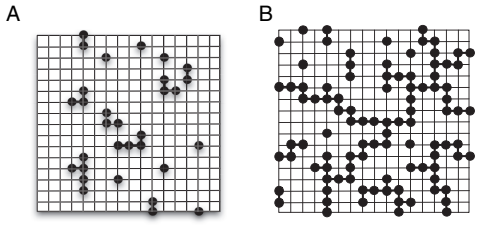

Fig. 6.3. Site percolation problem in two dimensions. Each lattice site is occupied (filled circles) with probability p. A, At small p, only small clusters of occupied sites are formed. B, At large p, a *percolating cluster* of occupied sites connects opposite boundaries.

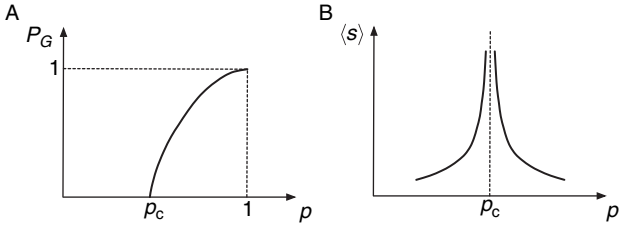

Fig. 6.4. A, Schematic plot of the probability P_G for a node to belong to the infinite percolating cluster as a function of the occupation probability p. For $p < p_c$, P_G is equal to zero in the thermodynamic limit, while it takes strictly positive values for $p > p_c$. B, Evolution of the average size of the finite clusters close to the transition.

probability p and $1 - p$ respectively, and is described by the same phenomenology of site percolation by increasing the percolation probability. As the size of the lattice goes to infinity, the change between the two possible behaviors sketched in Figure 6.3 defines a phase transition (see Chapter 5) at a critical value p_c. For $p < p_c$, all clusters have a finite size, while for $p > p_c$ a *giant* cluster appears and contains a finite fraction of all lattice sites, and thus becomes of infinite size in the thermodynamic limit corresponding to a system of infinite size. This allows us to generalize the concept of percolation transition to any kind of network.

In the percolation problem, the order parameter is defined as the probability P_G for a node to belong to the infinite percolating cluster, and evolves from 0 for $p \leq p_c$ to a finite value at $p > p_c$, as sketched in Figure 6.4. A basic quantity describing the system structure is the number $N_s(p)$ of clusters of size s in a network of size N, or as customarily used the *cluster number distribution* $n_s(p) = N_s(p)/N$, which is the number of clusters of size s per lattice vertex, at the percolation probability p. The probability for any node i to belong to a cluster of size s is simply given by $sn_s(p)$, where the fact that the vertex can be any one of the s cluster's elements has been considered. The probability p of a site to be occupied can then be rewritten

https://doi.org/10.1017/CBO9780511791383.007 Published online by Cambridge University Press

as the sum of these probabilities over all possible sizes. If $p < p_c$, this translates into

$$p = \sum_s s n_s(p). \tag{6.2}$$

Above the critical point p_c, the infinite cluster appears and each node has a finite probability $P_G > 0$ to be part of it. As any occupied vertex belongs either to the infinite cluster or to a cluster of finite size, we can write for $p > p_c$ that

$$p = P_G + \sum_s{}' s n_s(p), \tag{6.3}$$

where $\sum_s{}'$ indicates that the giant cluster is excluded from the summation.

The function $n_s(p)$ also allows writing the conditional probability that an occupied vertex belongs to a cluster of size s as $s n_s(p)/\sum_s{}' s\, n_s(p)$, where the infinite cluster has been excluded to avoid divergences. The average size $\langle s \rangle$ of the cluster to which any occupied vertex belongs is therefore given by

$$\langle s \rangle = \frac{\sum_s{}' s^2 n_s(p)}{\sum_s{}' s n_s(p)}, \tag{6.4}$$

where again the divergence due to the infinite clusters is not taken into account by considering the constrained sums $\sum_s{}'$. At $p < p_c$ the average cluster size $\langle s \rangle$ is finite. For increasing values of p the average size increases. At p_c the appearance of the giant cluster corresponds to the divergence of the average size that above p_c is completely contained in the infinite connected cluster excluded by the sum. It then results that $\langle s \rangle$ is a singular function at p_c, as shown in Figure 6.4. This divergence contains much physical information about the system and is the fingerprint of a critical phase transition. Indeed, the singularity at p_c corresponds to the lack of a characteristic length for the clusters which is at the origin of the scaling behavior typical of phase transitions (see Chapter 5) and yields the following scaling form for $n_s(p)$, close to the transition

$$n_s(p) = \begin{cases} s^{-\tau} f_+(s/s_c), & \text{if } p \geq p_c \\ s^{-\tau} f_-(s/s_c), & \text{if } p \leq p_c \end{cases} \quad \text{with } s_c = |p_c - p|^{-1/\sigma}, \tag{6.5}$$

where $f_+(x)$ and $f_-(x)$ are two scaling functions which converge to the same finite constant when $x \to 0$ ($f_+(0) = f_-(0)$), and have a fast decay (e.g. exponential) at large x. Here τ and σ are exponents whose values depend on the dimensionality and other properties of the system. The quantity $s_c(p)$, equivalent to the characteristic length in equilibrium phase transitions, plays the role of the size cut-off: only connected clusters with a size smaller or comparable to $s_c(p)$ are present and define the physical properties of the system for any given value of p.

https://doi.org/10.1017/CBO9780511791383.007 Published online by Cambridge University Press

Using the scaling form for $n_s(p)$ and replacing the sum by an integral in the numerator of Equation (6.4), one obtains for the average size of the finite clusters close to p_c the following relation

$$\langle s \rangle \sim \frac{1}{p} \int s^2 s^{-\tau} f(s/s_c) \mathrm{d}s \sim s_c^{3-\tau} \int x^{2-\tau} f(x) \mathrm{d}x \sim |p_c - p|^{(\tau-3)/\sigma}, \quad (6.6)$$

which predicts that the average size of finite clusters scales as a power law. Analogously, the probability for a node to be in the giant cluster P_G can be estimated close to p_c, by noting that $p_c = \sum_s s n_s(p_c)$ (since at $p = p_c$, $P_G = 0$), and rewriting Equation (6.3) for $p \approx p_c$ as

$$\begin{aligned} P_G &\approx \sum_s s[n_s(p_c) - n_s(p)] \sim \int \mathrm{d}s \, s^{1-\tau} [f(0) - f(s/s_c)] \\ &\sim s_c^{2-\tau} \sim (p - p_c)^{(\tau-2)/\sigma}. \end{aligned} \quad (6.7)$$

Note that in order for the sum $\sum_s s n_s(p_c)$ to converge, one needs $\tau > 2$, so that P_G goes to 0 as $p \to p_c$, as initially assumed.

From the scaling form for $n_s(p)$, it follows that both P_G and $\langle s \rangle$ obey the power-law scaling forms close to p_c

$$\langle s \rangle \sim |p_c - p|^{-\gamma}, \quad (6.8)$$

$$P_G \sim (p - p_c)^{\beta}, \quad (6.9)$$

which define the critical exponents $\gamma = (3 - \tau)/\sigma$ and $\beta = (\tau - 2)/\sigma$. The last two equations are the classical scaling relations customarily found in critical phenomena.

Percolation theory has been extensively validated for different kinds of lattices in both analytical and computer simulations studies (Stauffer and Aharony, 1992). The power-law behavior and singular functions found at the percolation threshold are a typical example of critical phase transition, where the onset of a macroscopically ordered phase (for instance the presence of a global connected structure) is anticipated by large fluctuations in the statistical properties of the system (Binney *et al.*, 1992). When these fluctuations become of the order of the system size itself, at the critical point, the macroscopic order arises and the system enters the new phase. In addition, as with equilibrium critical phenomena, percolation exhibits the universality of critical behavior and exponents. Indeed, the exact value of the critical exponents does not depend on the fine details of the percolation model. In general, they just depend on the system's dimensionality and symmetries of the order parameter. Thus, while the exact value of p_c depends on the lattice geometry, the critical exponents do not.

https://doi.org/10.1017/CBO9780511791383.007 Published online by Cambridge University Press

6.3 Percolation in complex networks

As described in the previous section, percolation phenomena are generally considered on regular lattices embedded in a D-dimensional space. In random graphs with N vertices, however, there is no embedding space and any vertex can in principle be connected to any other vertex. This is equivalent to working in a space which is $(N-1)$-dimensional where any vertex has $N-1$ possible neighbors. Depending on the graph connectivity properties, we may or may not observe a giant connected component made of a finite fraction of nodes.[1] In the $N \to \infty$ limit often considered in random graph theory, the problem is therefore analogous to infinite-dimensional edge percolation. In network language, the critical point thus translates unambiguously into the existence of a given threshold condition that marks the separation between a regime in which the network is fragmented into a myriad of small subgraphs and a regime in which there is a giant component containing a macroscopic fraction of the network's vertices.

The study of the percolation transition as a function of the connectivity properties of generalized random graphs finds a convenient formulation in the generating functions technique (see Callaway *et al.* [2000]; Newman [2003c] and Appendix 2). We report here a non-rigorous argument which provides the condition for a giant cluster to arise in graphs that have a local tree structure with no cycles. We focus for simplicity on undirected graphs, while the case of directed graphs is described in Appendix 3. We consider an uncorrelated network with degree distribution $P(k)$ and we denote by q the probability that a randomly chosen edge does not lead to a vertex connected to a giant cluster. This probability can be self-consistently computed if cycles are neglected. It can indeed be written as the average over all possible degrees k of the products of two probabilities: (i) the probability $kP(k)/\langle k\rangle$ that the randomly picked edge leads to a vertex of degree k (see Chapter 1); (ii) the probability q^{k-1} that none of the remaining $k-1$ edges lead to a vertex connected to a giant cluster. This translates into the self-consistent equation

$$q = \sum_k \frac{kP(k)}{\langle k\rangle} q^{k-1}. \tag{6.10}$$

The probability P_G for a given site to belong to a giant cluster can also be easily written: $1-P_G$ is the probability of *not* belonging to this cluster, which is, for a

[1] For instance, the onset of the giant component of the Erdős–Rényi random graph is analogous to an edge percolation problem in which the $N-1$ edges of each vertex can each be occupied with probability p.

https://doi.org/10.1017/CBO9780511791383.007 Published online by Cambridge University Press

node of degree k, the probability q^k that none of its edges lead to the giant cluster. We then obtain

$$P_G = 1 - \sum_k P(k) q^k. \tag{6.11}$$

The value $q = 1$, which is always a solution of Equation (6.10), corresponds to $P_G = 0$, i.e. to the absence of any percolating cluster. On the other hand, the percolation transition is determined by the appearance of another solution to Equation (6.10). The necessary condition for such a possibility can be determined in a simple graphical way as sketched in Figure 6.5. Indeed, we can rewrite Equation (6.10) as $q = F(q)$ with $F(q) = \sum_k k P(k) q^{k-1} / \langle k \rangle$. The function F has the following properties: $F(0) = P(1)/\langle k \rangle$, $F(1) = 1$, $F'(q) > 0$ and $F''(q) > 0$ for $0 < q < 1$, which implies that F is monotonously growing and convex. Figure 6.5 shows schematically the curve $y = F(q)$ together with the straight line $y = q$. It is clear that an intersection between these two lines exists at $q < 1$ if and only if the slope of F at $q = 1$ is larger than the slope of $y = q$. Mathematically this leads to the condition for the presence of a giant component

$$\frac{\mathrm{d}}{\mathrm{d}q} \left(\sum_k \frac{k P(k)}{\langle k \rangle} q^{k-1} \right) \Bigg|_{q=1} > 1, \tag{6.12}$$

which can be rewritten as

$$\frac{\langle k^2 \rangle}{\langle k \rangle} > 2. \tag{6.13}$$

The percolation condition (6.13), in which the heterogeneity parameter $\kappa = \langle k^2 \rangle / \langle k \rangle$ appears, is exact if cycles are statistically irrelevant, which is the case for random uncorrelated graphs in the $N \to \infty$ limit close to the transition point, and was first derived on more rigorous grounds by Molloy and Reed (1995). More precisely, it is also possible to show that the percolation threshold marks the critical point of a phase transition, separating the phase (for $\langle k^2 \rangle / \langle k \rangle < 2$) in which all the

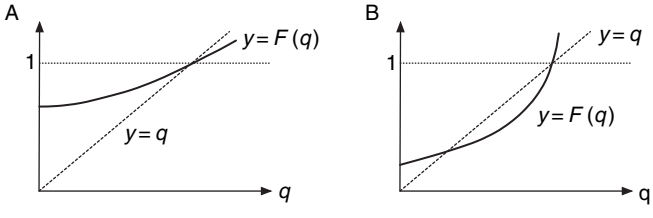

Fig. 6.5. Schematic graphical representation of Equation (6.10). A, The curves $y = F(q)$ and $y = q$ intersect only at $q = 1$. B, A second intersection with $q < 1$ is also obtained if and only if the slope of the function $F(q)$ in $q = 1$ is larger than 1.

https://doi.org/10.1017/CBO9780511791383.007 Published online by Cambridge University Press

components are trees and the size of the largest component scales at most as $\ln N$, from the phase (for $\langle k^2\rangle/\langle k\rangle > 2$) in which there exists a giant component of size proportional to N, while the sizes of the other components scale at most as $\ln N$. At the point $\langle k^2\rangle/\langle k\rangle = 2$, the largest cluster scaling is anomalous and follows the behavior $N^{2/3}$.

In this framework, the critical parameter is determined by the connectivity properties of the network. For instance, in the case of a Poisson random graph where $\langle k^2\rangle = \langle k\rangle^2 + \langle k\rangle$, the condition of Equation (6.13) takes the form $\langle k\rangle_c = 1$. This means that any Poisson random graph with average degree larger than 1 exhibits a giant component and $\langle k\rangle$ can be considered as the critical parameter. In the case of the Erdős–Rényi model, in which edges are drawn with probability p, the average degree is given by the expression $\langle k\rangle = pN$ and the critical connection probability $p_c = 1/N$ is recovered.

6.4 Damage and resilience in networks

In the percolation framework, the macroscopic behavior of networks in the case of random removal of vertices or edges finds a natural characterization in terms of an *inverse* percolation process in a connected random graph. In this context, the lattice in which percolation takes place is the graph under consideration. In the intact graph, with $f = 0$, all the vertices are occupied. The deletion of a fraction f of vertices corresponds to a random graph in which the vertices are occupied with probability $p = 1 - f$. For small f, we are in the region of p close to 1, in which the infinite cluster (identified as the giant component) is present. The threshold for the destruction of the giant component, $f_c = 1 - p_c$, can be thus computed from the percolation threshold at which the infinite cluster first emerges. In this case the phase transition corresponds to the separation of a region of damages where there still exists a connected network of appreciable size from a region in which the system is fragmented into small clusters. The order parameter P_G is a function of $f = 1 - p$ and can be defined as $P_G = S_f/S_0$, where as in the previous sections S_f is the size of the largest component after a damage f and $S_0 = N$ is the size of the original network.[2] The strategy for calculating the damage threshold thus consists in finding the damage density f_c at which the surviving network fulfills the percolation condition $\langle k^2\rangle_f/\langle k\rangle_f = 2$, where $\langle k^2\rangle_f$ and $\langle k\rangle_f$ refer to the degree distribution moments of the damaged graph.

[2] It is worth remarking, however, that only in the infinite size limit does the relation $P_G = \lim_{S_0\to\infty} S_f/S_0$ unambiguously define the transition point. In finite systems, the transition is smoother and the order parameter never attains a null value above the threshold, relaxing to its minimum value $P_G = 1/S_0$.

https://doi.org/10.1017/CBO9780511791383.007 Published online by Cambridge University Press

Starting from an undamaged network with degree distribution $P_0(k)$, average degree $\langle k\rangle_0$, and second moment $\langle k^2\rangle_0$, it is possible to compute the corresponding $P_f(k)$, $\langle k\rangle_f$ and $\langle k^2\rangle_f$ after the random removal of a fraction f of nodes (Cohen *et al.*, 2000). For each surviving node of initial degree k_0, the random removal amounts to the deletion of a certain number of its neighbors (each one independently with probability f), and the node has remaining degree k with probability

$$\binom{k_0}{k}(1-f)^k f^{k_0-k}. \tag{6.14}$$

The resulting degree distribution $P_f(k)$ is obtained by summing expression (6.14) over all possible values of k_0, each one weighted by its probability of appearance $P_0(k_0)$ in the initial network

$$P_f(k) = \sum_{k_0 \geq k} P_0(k_0) \binom{k_0}{k}(1-f)^k f^{k_0-k}. \tag{6.15}$$

One finally obtains $\langle k\rangle_f = (1-f)\langle k\rangle_0$ and $\langle k^2\rangle_f = (1-f)^2\langle k^2\rangle_0 + f(1-f)\langle k\rangle_0$. The critical value f_c is such that for $f > f_c$, no giant component can be found in the network. According to the Molloy and Reed criterion (6.13) obtained in the previous section, this occurs if and only if $\langle k^2\rangle_f < 2\langle k\rangle_f$, which can be rewritten as

$$f > 1 - \frac{\langle k\rangle_0}{\langle k^2\rangle_0 - \langle k\rangle_0}. \tag{6.16}$$

The critical value f_c is thus given by

$$\begin{aligned} f_c &= 1 - \frac{\langle k\rangle_0}{\langle k^2\rangle_0 - \langle k\rangle_0} \\ &= 1 - \frac{1}{\kappa - 1}, \end{aligned} \tag{6.17}$$

where $\kappa = \langle k^2\rangle_0/\langle k\rangle_0$ quantifies the heterogeneity of the initial network. This formula allows us to understand the different resilient behaviors exhibited by homogeneous and heterogeneous topologies. If the degree fluctuations are bounded, $\langle k^2\rangle_0$ is finite and f_c is strictly less than 1. As more nodes are removed, the size of the largest component thus decreases and reaches 0 when a certain fraction (strictly less than 1) of the nodes has disappeared. On the other hand, heavy-tailed networks display very large fluctuations and $\langle k^2\rangle_0$ diverges in the thermodynamic limit which leads to $f_c = 1$. This means that a giant component is present *for any fraction of removed sites strictly less than* 1. Random failures of an arbitrary fraction of the nodes therefore do not affect the functionality of the network. This extreme robustness is due to the presence of hubs which, although in small proportion, hold the

https://doi.org/10.1017/CBO9780511791383.007 Published online by Cambridge University Press

network together and are unlikely to be removed in the random process as small degree nodes are the huge majority.

The critical threshold derived above corresponds to the limit of infinite size. However, all real networks have a finite number of nodes N, so that the fluctuations $\langle k^2\rangle_0$ do not strictly diverge and f_c will not be strictly 1. Let us consider for concreteness the case of a scale-free network of size N, with degree distribution $P(k) = ck^{-\gamma}$ for $k = m, m+1, \ldots, k_c(N)$, where m is the minimum degree and c a normalization constant ($\gamma > 1$ in order to ensure convergence of $\int^{\infty} P(k)$). The cut-off $k_c(N)$ is the maximal degree observed in a system of size N and is given by the fact that typically only one node will have degree $k_c(N)$ or larger,[3] which can be written as

$$N \int_{k_c(N)}^{\infty} P(k)\mathrm{d}k = 1, \tag{6.18}$$

yielding $k_c(N) = mN^{1/(\gamma-1)}$. The ratio $\kappa = \langle k^2\rangle/\langle k\rangle$ can then easily be computed as

$$\kappa = \frac{2-\gamma}{3-\gamma} \cdot \frac{k_c(N)^{3-\gamma} - m^{3-\gamma}}{k_c(N)^{2-\gamma} - m^{2-\gamma}}, \tag{6.19}$$

leading to the different possible behaviors according to the value of γ:

- if $\gamma > 3$, $\kappa \sim (\gamma-2)m/(\gamma-3)$ is finite, so that f_c is strictly less than 1: a percolation threshold exists, just as for ordinary random graphs.
- if $\gamma < 3$, κ diverges as N goes to infinity ($\kappa \sim N^{(3-\gamma)/(\gamma-1)}$ if $2 < \gamma < 3$, and $\kappa \sim N^{1/(\gamma-1)}$ if $\gamma < 2$). The percolation threshold f_c therefore becomes closer and closer to 1 as N increases. Although, for any finite network, the size of the largest component goes to values close to 0 at a value of f_c smaller than 1, $1 - f_c$ is effectively small and the robustness increases as the initial network size increases.

In particular, for $2 < \gamma < 3$, which is encountered in many real networks, the threshold is given by

$$f_c \approx 1 - \frac{3-\gamma}{\gamma-2} m^{2-\gamma} k_c(N)^{\gamma-3}, \tag{6.20}$$

and is close to 1 even at relatively small network sizes. For example, for $N = 1000$, $m = 1$, $\gamma = 2.5$, one obtains $k_c = 100$ and $f_c \approx 0.9$.

The cut-off in the degree distribution can also arise because of some physical constraints. The physical Internet is an example of this, since the routers cannot be linked to an arbitrarily large number of other routers. In this case, the degree fluctuations do not diverge, even in the infinite size limit. A typical example of such degree distribution can be written as $P(k) = ck^{-\gamma}\exp(-k/k_c)$ ($2 < \gamma < 3$).

[3] See Appendix 1 for a detailed derivation of this result.

https://doi.org/10.1017/CBO9780511791383.007 Published online by Cambridge University Press

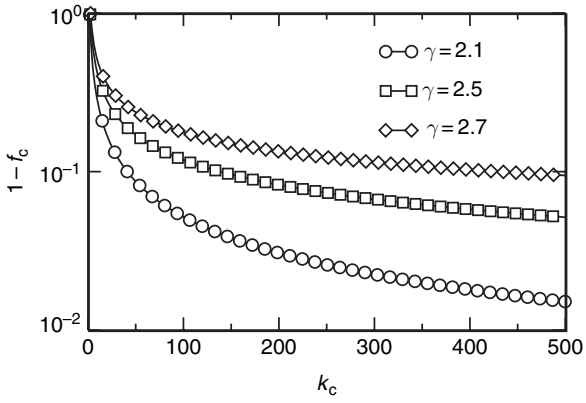

Fig. 6.6. Threshold for the random removal of vertices, for graphs with degree distribution of the form $P(k) = ck^{-\gamma}\exp(-k/k_c)$. The extension of the fragmented region $1 - f_c$, is plotted as a function of the cut-off k_c for various exponents γ. For $\gamma \leq 3$ f_c tends to 1 as k_c increases. Networks with lower exponents have a larger resilience to damage at given cut-off.

It is then possible to compute κ and f_c (Callaway *et al.*, 2000), obtaining that f_c tends to 1 as k_c increases, and this more and more rapidly as γ decreases, as shown in Figure 6.6.

Finally, we note that the theory presented so far refers to *uncorrelated* networks: the probabilities that two neighboring vertices have degree k and k', respectively, are independent. In fact, most real networks bear correlations, which are described by the conditional probability $P(k|k')$ that a node has degree k given that it is the neighbor of a node of degree k' (see Chapter 1). The behavior of the percolation transition and of the damage threshold then depend on the form of the correlations (Newman, 2002a; Moreno and Vázquez, 2003). It can in fact be shown that $f_c = 1 - 1/\Lambda$, where Λ is the largest eigenvalue of the *correlation matrix* having elements $C_{k'k} = (k-1)P(k|k')$. The resilience properties of a correlated network thus depend on the possible divergence of this eigenvalue. Generically, it turns out that it does diverge for heavy-tailed networks with divergent second moment (Boguñá, Pastor-Satorras and Vespignani, 2003b). For concreteness, one can state that, for finite networks in which f_c is always lower than 1, assortative networks in which high degree vertices tend to stick together are more resilient than disassortative networks.

6.5 Targeted attacks on large degree nodes

So far we have considered only random percolation models suited at best to simulate the occurrence of random failure. We have also discussed the behavior of

https://doi.org/10.1017/CBO9780511791383.007 Published online by Cambridge University Press

networks in the case of targeted attacks and it is interesting to explain this phenomenology in the framework of percolation phenomena. In order to do this we have to consider the percolation transition of the removal of nodes according to deterministic strategies.

Let us first consider that nodes are knocked out in the order defined by their degree rank; that is, the nodes are removed in descending order of degree centrality. In this case the analytical calculation has been worked out explicitly in generalized uncorrelated random networks with arbitrary degree distribution $P(k)$ (Callaway *et al.*, 2000; Cohen *et al.*, 2001). The removal of a fraction f of the highest degree nodes corresponds to the removal of all nodes of degree larger than a certain value $k_c(f)$, implicitly defined by the equation

$$f = \sum_{k=k_c(f)+1}^{\infty} P(k). \tag{6.21}$$

Moreover, such a removal will modify the degree distribution of the remaining nodes, owing to the deletion of the edges between removed and remaining nodes. The probability that one of the neighbors of any given node is removed equals the probability that the corresponding link points to a node of degree larger than $k_c(f)$, i.e.

$$r(f) = \sum_{k=k_c(f)+1}^{\infty} \frac{kP(k)}{\langle k \rangle}. \tag{6.22}$$

The surviving graph is thus equivalent to a network with cut-off $k_c(f)$, from which the neighbors of each node are randomly removed with probability $r(f)$. The Molloy and Reed criterion yields the following equation for the threshold value f_c at which the giant component disappears:

$$r(f_c) = 1 - \frac{1}{\kappa(f_c) - 1}, \tag{6.23}$$

where

$$\kappa(f_c) = \frac{\sum_k^{k_c(f_c)} k^2 P(k)}{\sum_k^{k_c(f_c)} kP(k)}. \tag{6.24}$$

Explicit values of the damage threshold can be calculated in scale-free graphs of minimum degree m and degree distribution $P(k) = ck^{-\gamma}$. By using the continuous degree approximation which replaces the sums by integrals in the various equations, we obtain

$$k_c(f) \approx mf^{1/(1-\gamma)}, \quad r(f) \approx f^{(2-\gamma)/(1-\gamma)}, \tag{6.25}$$

https://doi.org/10.1017/CBO9780511791383.007 Published online by Cambridge University Press

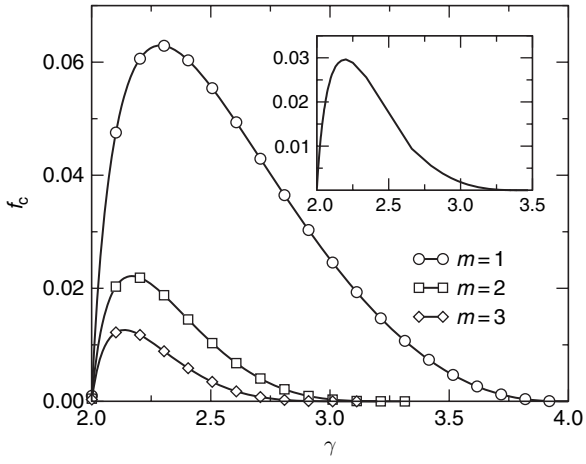

Fig. 6.7. Threshold f_c for the targeted removal of the most connected nodes, for scale-free graphs ($P(k) \sim k^{-\gamma}$) of minimum degree m, as a function of the exponent γ. The symbols correspond to an approximate computation treating the degrees as continuous variables (Cohen *et al.*, 2001), while the inset shows the results of the discrete formalism of Dorogovtsev and Mendes (2001), for $m = 1$.

and

$$\kappa(f_c) \approx \frac{2-\gamma}{3-\gamma} \times \frac{k_c^{3-\gamma} - m^{3-\gamma}}{k_c^{2-\gamma} - m^{2-\gamma}}. \tag{6.26}$$

Plugging these expressions into Equation (6.23) yields the implicit threshold condition

$$f_c^{(2-\gamma)/(1-\gamma)} = 2 + \frac{2-\gamma}{3-\gamma} m \left(f_c^{(3-\gamma)/(1-\gamma)} - 1 \right), \tag{6.27}$$

which can be solved numerically providing an estimate of f_c always of the order of a few percent for $\gamma \in [2, 3]$, as shown in Figure 6.7. Dorogovtsev and Mendes (2001) have in fact shown that a more rigorous approach can also be undertaken which treats the degrees as discrete variables, and that the obtained equation can be solved numerically. The results, shown in the inset of Figure 6.7, point to an even greater fragility since f_c is lower than in the continuous degree approximation. These results clearly show the fragility of heterogeneous networks where the removal of a very small fraction of the hubs is sufficient to shatter the network into small pieces and destroy its functionalities. The divergence of the degree fluctuations and the relative abundance of very high degree nodes appear again as the origin of the extreme fragility in front of targeted attacks of heavy-tailed networks.

The analytical results we have shown assume a perfect knowledge of the ranking of nodes in the network according to the degree centrality. Of course, in real-world large-scale networks it is very difficult to reach such a global knowledge of the

https://doi.org/10.1017/CBO9780511791383.007 Published online by Cambridge University Press

connectivity pattern, and intermediate targeting strategies have been investigated (Gallos *et al.*, 2004; 2005) in which the probability to remove a node of degree k is proportional to k^{α}. The limits $\alpha = 0$ and $\alpha \to \infty$ then represent, respectively, random removal and deterministic attacks on the most connected nodes. As could be intuitively expected, it turns out that the critical point f_c at which the network becomes disconnected increases as α decreases: for a given fraction of nodes undergoing a failure, larger probabilities that these removed nodes are hubs lead to smaller remaining connected components.

6.5.1 Alternative ranking strategies

As already stated, the most intuitive topological measure of importance (and centrality) of a node is given by its degree. However, by considering solely the degree of a node we overlook that nodes with small degree may be crucial for connecting different regions of the network by acting as bridges. With this in mind, a detailed study of the effects of various attack strategies on heterogeneous real-world as well as on model networks has been realized by Holme *et al.* (2002). In particular, the effect of targeting nodes with largest degree has been compared with the removal of nodes with the largest betweenness centrality.

In many model networks, such as the Barabási–Albert model, betweenness centrality and degree are in fact strongly correlated, and in particular the most connected nodes typically coincide with the most central ones (see Chapter 1). The two types of attacks thus yield very similar effects. In many real-world networks, however, the situation is more complex: although centrality and degree are always correlated, large fluctuations are often observed and some nodes may have large betweenness centrality despite a relatively modest degree. Such features have been uncovered, for example in the worldwide airport network (see Chapter 2), and appear generically in networks where the tendency to form hubs is contrasted by geographical constraints (Barrat *et al.*, 2005).

Another important consideration is taken into account by Holme *et al.* (2002): each time a node is removed, the next on the list in order of decreasing degree or betweenness centrality may in fact change. This is particularly clear for the betweenness centrality since the removal of one node alters the routes of the shortest paths and thus may affect the betweenness of all nodes. As a result, four different attack strategies can be considered: (i) removing the nodes in decreasing order of degree according to the *initial* list of degrees, or (ii) the *initial* list of betweenness centralities, or according after each removal to the (iii) *recalculated* list of degrees (RD) or (iv) the *recalculated* list of betweenness centralities (RB).

Systematically, it turns out that the RB strategy is the most lethal for the network (see Figure 6.8 A for a comparison of RD and RB). This is quite understandable

https://doi.org/10.1017/CBO9780511791383.007 Published online by Cambridge University Press

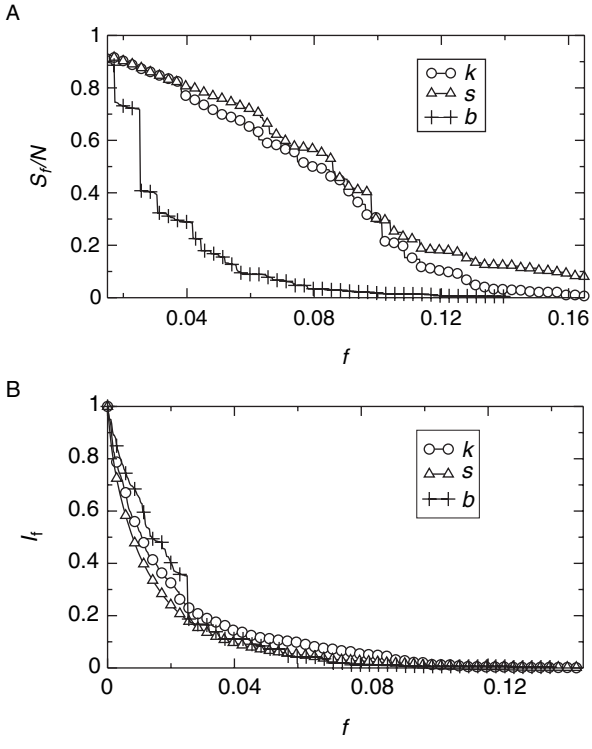

Fig. 6.8. Effect of different node removal strategies on the structure of the worldwide airport network. Nodes are removed in order of decreasing degree k, strength s or betweenness centrality b. A, Decrease of the size of the largest connected component. B, Decrease of the network's integrity I_f defined as the largest traffic or strength still carried by a connected component of the network, divided by the initial total strength of the undamaged network. Data from Dall'Asta *et al.* (2006c).

since at each step, the node through which the largest number of shortest paths goes is removed. For comparison, the result of the same attacks on homogeneous graphs is much less dramatic: the absence of hubs makes a network more resilient to targeted attacks since all nodes have approximately the same importance. Analogous results have been obtained in the case of the North American power grid which displays simultaneously an exponentially decaying degree distribution and strong heterogeneities in the betweenness centrality (Albert, Albert and Nakarado, 2004). Finally, another interesting point made by Holme *et al.* (2002) is that for a given average degree, large clustering values renders the network more vulnerable. This can be intuitively understood by considering that the edges creating triangles are locally redundant but are not used for holding together distant parts of the network.

https://doi.org/10.1017/CBO9780511791383.007 Published online by Cambridge University Press

6.5.2 Weighted networks

In real networks, complex topological features are often associated with a diversity of interactions as measured by the weights of the links. In order to study the vulnerability of such networks to intentional attacks, these attributes must therefore be considered along with the topological quantities. Recent works have indeed proposed centrality measures and damage indicators which take into account the links' weights or capacities. The *integrity* (Dall'Asta *et al.*, 2006c) of a damaged network is defined as the largest traffic or strength still carried by a connected component of the network, divided by the initial total strength of the undamaged network. Its study as a function of the fraction of nodes provides interesting complementary information on the vulnerability of complex networks. While the theory of inhomogeneous percolation can be used to generalize the Molloy–Reed criterion to weighted networks (Dall'Asta, 2005), we will employ the example of the worldwide airport network to demonstrate the effects of various kinds of malicious attacks. Figure 6.8 illustrates the decrease of the size of the largest connected component, for various attack strategies, as well as the decay of the integrity of the network. As expected, all strategies lead to a rapid breakdown of the network with a very small fraction of removed nodes. Moreover, in agreement with the results on unweighted networks (Holme *et al.*, 2002), the size of the giant component decreases faster upon removal of nodes which are identified as central according to global properties (i.e. betweenness), instead of local ones (i.e. degree, strength). Interestingly, when the attention shifts to the behavior of the integrity measure, one finds a different picture in which all the strategies achieve the same level of damage. Most importantly, its decrease is even faster and more pronounced than for topological quantities: for S_f/N still of the order of 80%, the integrity is typically smaller than 20%. This emphasizes how the purely topological measure of the size of the largest component does not convey all the information needed. In other words, the functionality of the network can be temporarily jeopardized in terms of traffic even if the physical structure is still globally well connected. This implies that weighted networks appear to be more fragile than thought by considering only topological properties. All targeted strategies are very effective in dramatically damaging the network, and reach the complete destruction at a very small threshold value of the fraction of removed nodes.

As discussed in the previous section, attacks based on initial centrality ranking lead to smaller *topological* damage compared with the case where the centrality measure (degree or betweenness) is recalculated after each node removal. However, when traffic integrity measures are studied, differences are negligible: a very fast decrease of the integrity is observed for all strategies, based either on initial or recalculated quantities.

https://doi.org/10.1017/CBO9780511791383.007 Published online by Cambridge University Press

In summary, the study of the vulnerability of weighted networks to various targeted attack strategies has shown that complex networks are more fragile than expected from the analysis of topological quantities when the traffic characteristics are taken into account. In particular, the network's integrity in terms of carried traffic is vanishing significantly before the network is topologically fragmented. Moreover, the integrity of the network is harmed in a very similar manner by attacks based on initial or recalculated centrality rankings. All these results warn about the extreme vulnerability of the traffic properties of weighted networks and signal the need to pay particular attention to weights and traffic in the design of protection strategies.

6.6 Damage in real-world networks

The percolation model is a very stylized model of networks' reactions to local damage and clearly does not capture most of the features contributing to the resilience and robustness of real-world networks. It would be a gross oversimplification to conclude that what is presented in this chapter may explain a real blackout or internet congestion.

First of all, we have presented a purely topological picture. As the network is progressively damaged by the removal of nodes, its topology is modified, and in particular some node characteristics depending on the whole structure, such as the betweenness centrality, may change strongly, as mentioned in Section 6.5. This naturally leads to the concept of cascading failures: the failure of a single node leads to a redistribution of traffic on the network which may trigger subsequent overloads and failure of the next most-loaded node. While avalanche and cascading phenomena will be analyzed in Chapter 11, another main issue of real-world networks is not at all considered. As we discussed in the early chapters of the book, the network models we use are generally unstructured. They are good at capturing large-scale statistical properties but do not take into account the inherent level of local engineering of most of the real-world infrastructures. In addition, engineering in most cases is aimed at reducing risk and damage spreading in actual failure occurrence.

On the other hand, it would be inconclusive to approach the problem of network robustness in a "deterministic" way focusing only on the technical engineering and the (ubiquitous) human error. In particular the stylized approaches presented here show that, on the large scale, the inherent complexity of our infrastructures has built-in critical response properties to local damages which may be responsible for large-scale failures. In other words, we need to capitalize conceptually on these simple models by introducing higher levels of realism that might tackle at once the engineering and the globally emerging properties in risk evaluation and prediction.

https://doi.org/10.1017/CBO9780511791383.007 Published online by Cambridge University Press