8

ALBERT-LÁSZLÓ BARABÁSI

NETWORK SCIENCE
NETWORK ROBUSTNESS

ACKNOWLEDGEMENTS

MÁRTON PÓSFAI
GABRIELE MUSELLA
NICOLE SAMAY
ROBERTA SINATRA
SARAH MORRISON
AMAL HUSSEINI
PHILIPP HOEVEL

INDEX

Figure 8.0 (cover image)
Networks & Art: Facebook Users

Created by Paul Butler, a Toronto-based data scientist during a Facebook internship in 2010, the image depicts the network connecting the users of the social network company. It highlights the links within and across continents. The presence of dense local links in the U.S., Europe and India is just as revealing as the lack of links in some areas, like China, where the site is banned, and Africa, reflecting a lack of Internet access.

PDF V26, 05.09.2014

INTRODUCTION

Errors and failures can corrupt all human designs: The failure of a component in your car's engine may force you to call for a tow truck or a wiring error in your computer chip can make your computer useless. Many natural and social systems have, however, a remarkable ability to sustain their basic functions even when some of their components fail. Indeed, while there are countless protein misfolding errors and missed reactions in our cells, we rarely notice their consequences. Similarly, large organizations can function despite numerous absent employees. Understanding the origins of this robustness is important for many disciplines:

- Robustness is a central question in biology and medicine, helping us understand why some mutations lead to diseases and others do not.
- It is of concern for social scientists and economists, who explore the stability of human societies and institutions in the face of such disrupting forces as famine, war, and changes in social and economic order.
- It is a key issue for ecologists and environmental scientists, who seek to predict the failure of an ecosystem when faced with the disruptive effects of human activity.
- It is the ultimate goal in engineering, aiming to design communication systems, cars, or airplanes that can carry out their basic functions despite occasional component failures.

Networks play a key role in the robustness of biological, social and technological systems. Indeed, a cell's robustness is encoded in intricate regulatory, signaling and metabolic networks; the society's resilience cannot be divorced from the interwoven social, professional, and communication web behind it; an ecosystem's survivability cannot be understood without a careful analysis of the food web that sustains each species. Whenever nature seeks robustness, it resorts to networks.

Figure 8.1
Achilles' Heel of Complex Networks

The cover of the 27 July 2000 issue of *Nature*, highlighting the paper entitled *Attack and error tolerance of complex networks* that began the scientific exploration of network robustness [1].

The purpose of this chapter is to understand the role networks play in ensuring the robustness of a complex system. We show that the structure of the underlying network plays an essential role in a system's ability to survive random failures or deliberate attacks. We explore the role of networks in the emergence of cascading failures, a damaging phenomenon frequently encountered in real systems. Most important, we show that the laws governing the error and attack tolerance of complex networks and the emergence of cascading failures, are universal. Hence uncovering them helps us understand the robustness of a wide range of complex systems.

Figure 8.2
Robust, Robustness

"Robust" comes from the latin Quercus Robur, meaning oak, the symbol of strength and longevity in the ancient world. The tree in the figure stands near the Hungarian village Diósviszló and is documented at www.dendromania.hu, a site that catalogs Hungary's oldest and largest trees.

Image courtesy of György Pósfai.

PERCOLATION THEORY

The removal of a single node has only limited impact on a network's integrity (Figure 8.3a). The removal of several nodes, however, can break a network into several isolated components (Figure 8.3d). Obviously, the more nodes we remove, the higher are the chances that we damage a network, prompting us to ask: How many nodes do we have to delete to fragment a network into isolated components? For example, what fraction of Internet routers must break down so that the Internet turns into clusters of computers that are unable to communicate with each other? To answer these questions, we must first familiarize ourselves with the mathematical underpinnings of network robustness, offered by *percolation theory*.

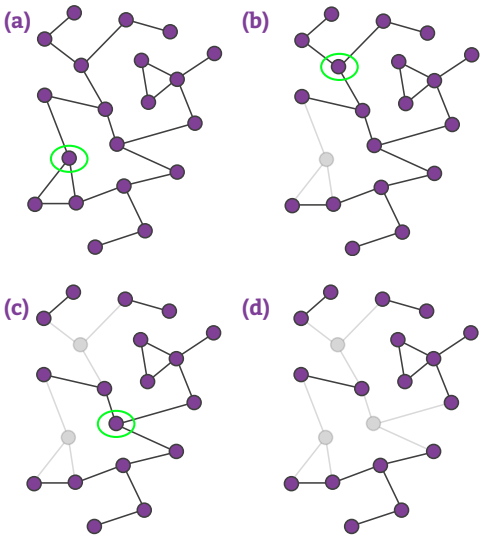


Figure 8.3
The Impact of Node Removal

The gradual fragmentation of a small network following the breakdown of its nodes. In each panel we remove a different node (highlighted with a green circle), together with its links. While the removal of the first node has only limited impact on the network's integrity, the removal of the second node isolates two small clusters from the rest of the network. Finally, the removal of the third node fragments the network, breaking it into five non-communicating clusters of sizes $s = 2, 2, 2, 5, 6$.

Percolation

Percolation theory is a highly developed subfield of statistical physics and mathematics [2, 3, 4, 5]. A typical problem addressed by it is illustrated in Figure 8.4a,b, showing a square lattice, where we place pebbles with probability p at each intersection. Neighboring pebbles are considered connected, forming clusters of size two or more. Given that the position of each pebble is decided by chance, we ask:

- What is the expected size of the largest cluster?
- What is the average cluster size?

Obviously, the higher is p, the larger are the clusters. A key prediction of percolation theory is that the cluster size does not change gradually with p. Rather, for a wide range of p the lattice is populated with numerous tiny clusters (Figure 8.4a). If p approaches a critical value p_c, these small clusters grow and coalesce, leading to the emergence of a large cluster at p_c. We call this the *percolating cluster* as it reaches the end of the lattice. In other words, at p_c we observe a phase transition from many small clusters to a percolating cluster that percolates the whole lattice (Figure 8.4b).

To quantify the nature of this phase transition, we focus on three quantities:

- **Average Cluster Size:** $\langle s \rangle$

  According to percolation theory the average size of all finite clusters follows

$$\langle s \rangle \sim |p - p_c|^{-\gamma_p} \tag{8.1}$$

  In other words, the average cluster size diverges as we approach p_c (Figure 8.4c).

- **Order Parameter:** P_∞

  The probability P_∞ that a randomly chosen pebble belongs to the largest cluster follows

$$P_\infty \sim (p - p_c)^{\beta_p}. \tag{8.2}$$

  Therefore as p decreases towards p_c the probability that a pebble belongs to the largest cluster drops zero (Figure 8.4d).

- **Correlation Length:** ξ

  The mean distance between two pebbles that belong to the same cluster follows

$$\xi \sim |p - p_c|^{-\nu}. \tag{8.3}$$

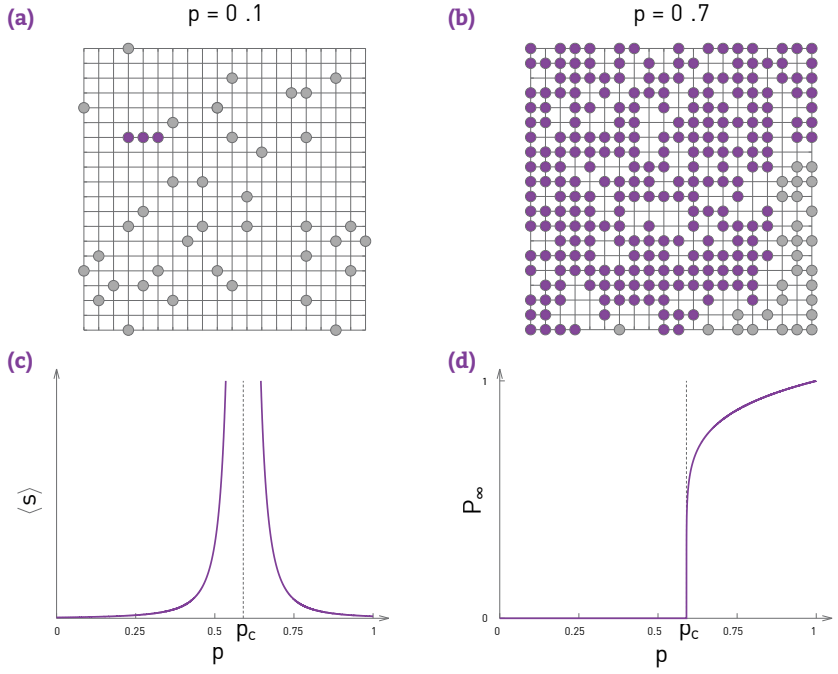


Figure 8.4
Percolation

A classical problem in percolation theory explores the random placement with probability p of pebbles on a square lattice.

(a) For small p most pebbles are isolated. In this case the largest cluster has only three nodes, highlighted in purple.

(b) For large p most (but not all) pebbles belong to a single cluster, colored purple. This is called the *percolating cluster*, as it spans the whole lattice (see also Figure 8.6).

(c) The average cluster size, $\langle s \rangle$, in function of p. As we approach p_c from below, numerous small clusters coalesce and $\langle s \rangle$ diverges, following (8.1). The same divergence is observed above p_c, where to calculate $\langle s \rangle$ we remove the percolating cluster from the average. The same exponent γ_p characterizes the divergence on both sides of the critical point.

(d) A schematic illustration of the p–dependence of the probability P_∞ that a pebble belongs to the largest connected component. For $p < p_c$ all components are small, so P_∞ is zero. Once p reaches p_c a giant component emerges. Consequently beyond p_c there is a finite probability that a node belongs to the largest component, as predicted by (8.2).

Therefore while for $p < p_c$ the distance between the pebbles in the same cluster is finite, at p_c this distance diverges. This means that at p_c the size of the largest cluster becomes infinite, allowing it to percolate the whole lattice.

The exponents γ_p, β_p, and ν are called *critical exponents*, as they characterize the system's behavior near the critical point p_c. Percolation theory predicts that these exponents are *universal*, meaning that they are independent of the nature of the lattice or the precise value of p_c. Therefore, whether we place the pebbles on a triangular or a hexagonal lattice, the behavior of $\langle s \rangle$, P_∞, and ξ is characterized by the same γ_p, β_p, and ν exponents.

Consider the following examples to better understand this universality:

- The value of p_c depends on the lattice type, hence it is not universal. For example, for a two-dimensional square lattice (Figure 8.4) we have $p_c \approx 0.593$, while for a two-dimensional triangular lattice $p_c = 1/2$ (site percolation).

- The value of p_c also changes with the lattice dimension: for a square lattice $p_c \approx 0.593$ ($d = 2$); for a simple cubic lattice ($d = 3$) $p_c \approx 0.3116$. Therefore in $d = 3$ we need to cover a smaller fraction of the nodes with pebbles to reach the percolation transition.

- In contrast with p_c, the critical exponents do not depend on the lattice type, but only on the lattice dimension. In two dimensions, the case shown in Figure 8.4, we have $\gamma_p = 43/18$, $\beta_p = 5/36$, and $\nu = 4/3$, for any lattice. In three dimensions $\gamma_p = 1.80$, $\beta_p = 0.41$, and $\nu = 0.88$. For any $d > 6$ we have $\gamma_p = 1$, $\beta_p = 1$, $\nu = 1/2$, hence for large d the exponents are independent of d as well [2].

Inverse Percolation Transition and Robustness

The phenomena of primary interest in robustness is the impact of node failures on the integrity of a network. We can use percolation theory to describe this process.

Let us view a square lattice as a network whose nodes are the intersections (Figure 8.5). We randomly remove an f fraction of nodes, asking how their absence impacts the integrity of the lattice.

If f is small, the missing nodes do little damage to the network. Increasing f, however, can isolate chunks of nodes from the giant component. Finally, for sufficiently large f the giant component breaks into tiny disconnected components (Figure 8.5).

This fragmentation process is not gradual, but it is characterized by a critical threshold f_c: For any $f < f_c$ we continue to have a giant component. Once f exceeds f_c, the giant component vanishes. This is illustrated by the f-dependence of P_∞, representing the probability that a node is part of the

giant component (Figure 8.5): P_∞ is nonzero under f_c, but it drops to zero as we approach f_c. The critical exponents characterizing this breakdown, γ_p, β_p, ν, are the same as those encountered in (8.1)-(8.3). Indeed, the two processes can be mapped into each other by choosing $f = 1 - p$.

What, however, if the underlying network is not as regular as a square lattice? As we will see in the coming sections, the answer depends on the precise network topology. Yet, for random networks the answer continues to be provided by percolation theory: Random networks under random node failures share the same scaling exponents as infinite-dimensional percolation. Hence the critical exponents for a random network are $\gamma_p = 1$, $\beta_p = 1$ and $\nu = 1/2$, corresponding to the $d > 6$ percolation exponents encountered earlier. The critical exponents for a scale-free network are provided in ADVANCED TOPICS 8.A.

In summary, the breakdown of a network under random node removal is not a gradual process. Rather, removing a small fraction of nodes has only limited impact on a network's integrity. But once the fraction of removed nodes reaches a critical threshold, the network abruptly breaks into disconnected components. In other words, random node failures induce a phase transition from a connected to a fragmented network. We can use the tools of percolation theory to characterize this transition in both regular and in random networks. For scale-free networks key aspects of the described phenomena change, however, as we discuss in the next section.

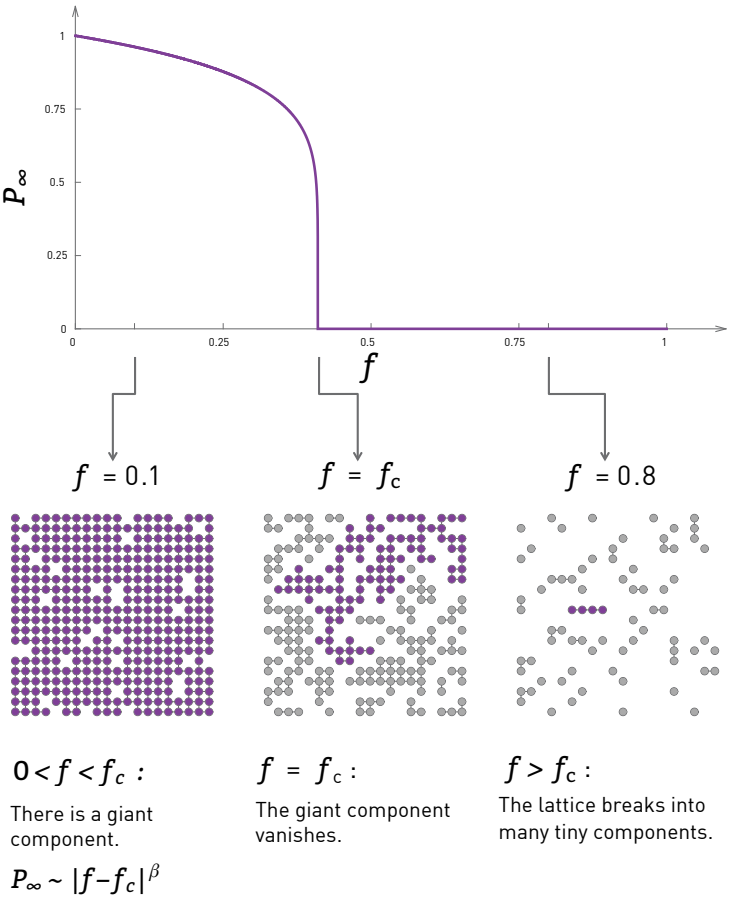


Figure 8.5
Network Breakdown as Inverse Percolation

The consequences of node removal are accurately captured by the inverse of the percolation process discussed in Figure 8.4. We start from a square lattice, that we view as a network whose nodes are the intersections. We randomly select and remove an f fraction of nodes and measure the size of the largest component formed by the remaining nodes. This size is accurately captured by P_∞, which is the probability that a randomly selected node belongs to the largest component. The observed networks are shown on the bottom panels. Under each panel we list the characteristics of the corresponding phases.

BOX 8.1

From Forest Fires to Percolation Theory

We can use the spread of a fire in a forest to illustrate the basic concepts of percolation theory. Let us assume that each pebble in Figure 8.4a,b is a tree and that the lattice describes a forest. If a tree catches fire, it ignites the neighboring trees; these, in turn ignite their neighbors. The fire continues to spread until no burning tree has a non-burning neighbor. We must therefore ask: If we randomly ignite a tree, what fraction of the forest burns down? And how long it takes the fire to burn out?

The answer depends on the tree density, controlled by the parameter p. For small p the forest consists of many small islands of trees (p = 0.55, Figure 8.6a), hence igniting any tree will at most burn down one of these small islands. Consequently, the fire will die out quickly. For large p most trees belong to a single large cluster, hence the fire rapidly sweeps through the dense forest (p = 0.62, Figure 8.6c).

The simulations indicate that there is a critical p_c at which it takes extremely long time for the fire to end. This p_c is the critical threshold of the percolation problem. Indeed, at $p = p_c$ the giant component just emerges through the union of many small clusters (Figure 8.6b). Hence the fire has to follow a long winding path to reach all trees in the loosely connected clusters, which can be rather time consuming.

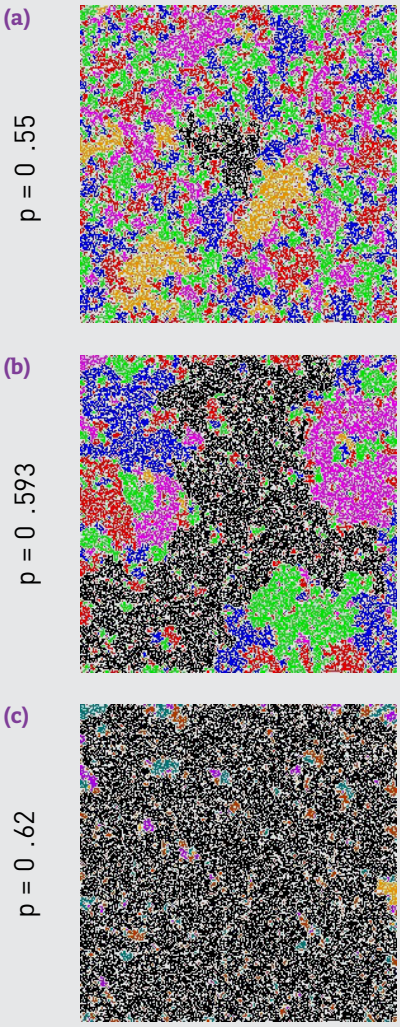


Figure 8.6
Forest Fire

The emergence of the giant component as we change the occupation probability p. Each panel corresponds to a different p in the vicinity of p_c shown for a lattice of 250x250 sites. The largest cluster is colored black. For $p < p_c$ the largest cluster is tiny, as seen in (a). If this is a forest and the pebbles are trees, any fire can at most consume only a small fraction of the trees, burning out quickly. Once p reaches $p_c \approx 0.593$, shown on (b), the largest cluster percolates the whole lattice and the fire can reach many trees, burning slowly through the forest. Increasing p beyond p_c connects more pebbles (trees) to the largest component, as seen for p = 0.62 on (c). Hence, the fire can sweep through the forest, burning out quickly again.

ROBUSTNESS OF SCALE-FREE NETWORKS

Percolation theory focuses mainly on regular lattices, whose nodes have identical degrees, or on random networks, whose nodes have comparable degrees. What happens, however, if the network is scale-free? How do the hubs affect the percolation transition?

To answer these questions, let us start from the router level map of the Internet and randomly select and remove nodes one-by-one. According to percolation theory once the number of removed nodes reaches a critical value f_c, the Internet should fragment into many isolated subgraphs (Figure 8.5). The simulations indicate otherwise: The Internet refuses to break apart even under rather extensive node failures. Instead the size of the largest component decreases gradually, vanishing only in the vicinity of $f = 1$ (Figure 8.7a). This means that the network behind the Internet shows an unusual robustness to random node failures: we must remove all of its nodes to destroy its giant component. This conclusion disagrees with percolation on lattices, which predicts that a network must fall apart after the removal of a finite fraction of its nodes.

The behavior observed above is not unique to the Internet. To show this we repeated the above measurement for a scale-free network with degree exponent $\gamma = 2.5$, observing an identical pattern (Figure 8.7b): Under random node removal the giant component fails to collapse at some finite f_c, but vanishes only gradually near $f = 1$ (Online Resource 8.1). This hints that the Internet's observed robustness is rooted in its scale-free topology. The goal of this section is to uncover and quantify the origin of this remarkable robustness.

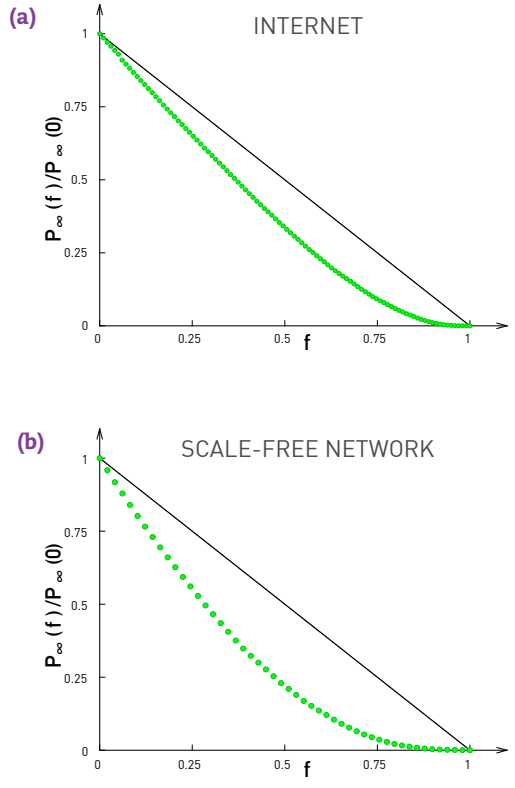


Figure 8.7
Robustness of Scale-free Networks

(a) The fraction of Internet routers that belong to the giant component after an f fraction of routers are randomly removed. The ratio $P_\infty(f)/P_\infty(0)$ provides the relative size of the giant component. The simulations use the router level Internet topology of Table 4.1.

(b) The fraction of nodes that belong to the giant component after an f fraction of nodes are removed from a scale-free network with $\gamma = 2.5$, $N = 10{,}000$ and $k_{min} = 1$.

The plots indicate that the Internet and in general a scale-free network do not fall apart after the removal of a finite fraction of nodes. We need to remove almost all nodes (i.e. f_c=1) to fragment these networks.

Molloy-Reed Criterion

To understand the origin of the anomalously high f_c characterizing the Internet and scale-free networks, we calculate f_c for a network with an arbitrary degree distribution. To do so we rely on a simple observation: For a network to have a giant component, most nodes that belong to it must be connected to at least two other nodes (Figure 8.8). This leads to the *Molloy-Reed criterion* (ADVANCED TOPICS 8.B), stating that a randomly wired network has a giant component if [6]

$$\kappa = \frac{\langle k^2 \rangle}{\langle k \rangle} > 2. \tag{8.4}$$

Networks with $\kappa < 2$ lack a giant component, being fragmented into many disconnected components. The Molloy-Reed criterion (8.4) links the network's integrity, as expressed by the presence or the absence of a giant component, to $\langle k \rangle$ and $\langle k^2 \rangle$. It is valid for any degree distribution p_k.

To illustrate the predictive power of (8.4), let us apply it to a random network. As in this case $\langle k^2 \rangle = \langle k \rangle(1 + \langle k \rangle)$, a random network has a giant component if

$$\kappa = \frac{\langle k^2 \rangle}{\langle k \rangle} = \frac{\langle k \rangle(1+\langle k \rangle)}{\langle k \rangle} = 1 + \langle k \rangle > 2 \tag{8.5}$$

or

$$\langle k \rangle > 1 . \tag{8.6}$$

This prediction coincides with the necessary condition (3.10) for the existence of a giant component.

Critical Threshold

To understand the mathematical origin of the robustness observed in Figure 8.7, we ask at what threshold will a scale-free network loose its giant component. By applying the Molloy-Reed criteria to a network with an arbitrary degree distribution, we find that the critical threshold follows [7] (ADVANCED TOPICS 8.C)

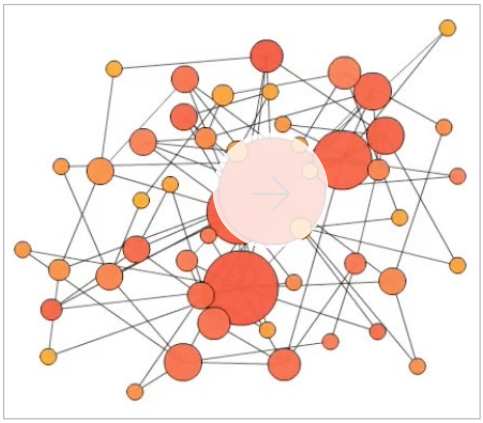
$$f_c = 1 - \frac{1}{\frac{\langle k^2 \rangle}{\langle k \rangle} - 1} . \tag{8.7}$$

The most remarkable prediction of (8.7) is that the critical threshold f_c depends only on $\langle k \rangle$ and $\langle k^2 \rangle$, quantities that are uniquely determined by the degree distribution p_k.

Let us illustrate the utility of (8.7) by calculating the breakdown threshold of a random network. Using $\langle k^2 \rangle = \langle k \rangle(\langle k \rangle + 1)$, we obtain (ADVANCED TOPICS 8.D)

$$f_c^{\mathrm{ER}} = 1 - \frac{1}{\langle k \rangle} . \tag{8.8}$$

Hence, the denser is a random network, the higher is its f_c, i.e. the more



Online Resource 8.1
Scale-free Network Under Node Failures

To illustrate the robustness of a scale-free network we start from the network we constructed in Online Resource 4.1, i.e. a scale-free network generated by the Barabási-Albert model. Next we randomly select and remove nodes one-by-one. As the movie illustrates, despite the fact that we remove a significant fraction of the nodes, the network refuses to break apart. Visualization by Dashun Wang.

Figure 8.8
Molloy-Reed Criterion

Each individual must hold the hand of two other individuals to form a chain. Similarly, to have a giant component in a network, on average each of its nodes should have at least two neighbors. The Molloy-Reed criterion (8.4) exploits this property, allowing us to calculate the critical point at which a network breaks apart. See ADVANCED TOPICS 8.B for the derivation.

nodes we need to remove to break it apart. Furthermore (8.8) predicts that f_c is always finite, hence a random network must break apart after the removal of a finite fraction of nodes.

Equation (8.7) helps us understand the roots of the enhanced robustness observed in Figure 8.7. Indeed, for scale-free networks with $\gamma < 3$ the second moment $\langle k^2 \rangle$ diverges in the $N \to \infty$ limit. If we insert $\langle k^2 \rangle \to \infty$ into (8.7), we find that f_c converges to $f_c = 1$. This means that *to fragment a scale-free network we must remove all of its nodes*. In other words, the random removal of a finite fraction of its nodes does not break apart a large scale-free network.

To better understand this result we express $\langle k \rangle$ and $\langle k^2 \rangle$ in terms of the parameters characterizing a scale-free network: the degree exponent γ and the minimal and maximal degrees, k_{min} and k_{max}, obtaining

$$f_c = \begin{cases} 1 - \dfrac{1}{\dfrac{\gamma-2}{3-\gamma} k_{min}^{\gamma-2} k_{max}^{3-\gamma} - 1} & 2 < \gamma < 3 \\ 1 - \dfrac{1}{\dfrac{\gamma-2}{\gamma-3} k_{min} - 1} & \gamma > 3 \end{cases} \tag{8.9}$$

Equation (8.9) predicts that (Figure 8.9):

- For $\gamma > 3$ the critical threshold f_c depends only on γ and k_{min}, hence f_c is independent of the network size N. In this regime a scale-free network behaves like a random network: it falls apart once a finite fraction of its nodes are removed.

- For $\gamma < 3$ the k_{max} diverges for large N, following (4.18). Therefore in the $N \to \infty$ limit (8.9) predicts $f_c \to 1$. In other words, to fragment an infinite scale-free network we must remove all of its nodes.

Equations (8.6)-(8.9) are the key results of this chapter, predicting that scale-free networks can withstand an arbitrary level of random failures without breaking apart. The hubs are responsible for this remarkable robustness. Indeed, random node failures by definition are blind to degree, affecting with the same probability a small or a large degree node. Yet, in a scale-free network we have far more small degree nodes than hubs. Therefore, random node removal will predominantly remove one of the numerous small nodes as the chances of selecting randomly one of the few large hubs is negligible. These small nodes contribute little to a network's integrity, hence their removal does little damage.

Returning to the airport analogy of Figure 4.6, if we close a randomly selected airport, we will most likely shut down one of the numerous small airports. Its absence will be hardly noticed elsewhere in the world: you can still travel from New York to Tokyo, or from Los Angeles to Rio de Janeiro.

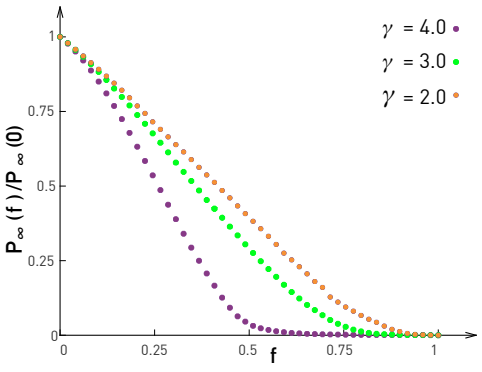


Figure 8.9
Robustness and Degree Exponent

The probability that a node belongs to the giant component after the removal of an f fraction of nodes from a scale-free network with degree exponent γ. For $\gamma = 4$ we observe a finite critical point $f_c \approx 2/3$, as predicted by (8.9). For $\gamma < 3$, however, $f_c \to 1$. The networks were generated with the configuration model using $k_{min} = 2$ and $N = 10,000$.

Robustness of Finite Networks

Equation (8.9) predicts that for a scale-free network f_c converges to one only if $k_{max} \to \infty$, which corresponds to the $N \to \infty$ limit. While many networks of practical interest are very large, they are still finite, prompting us to ask if the observed anomaly is relevant for finite networks. To address this we insert (4.18) into (8.9), obtaining that f_c depends on the network size N as (ADVANCED TOPICS 8.C)

$$f_c \approx 1 - \frac{C}{N^{\frac{3-\gamma}{\gamma-1}}}, \tag{8.10}$$

where C collects all terms that do not depend on N. Equation (8.10) indicates that the larger a network, the closer is its critical threshold to $f_c = 1$.

To see how close f_c can get to the theoretical limit $f_c = 1$, we calculate f_c for the Internet. The router level map of the Internet has $\langle k^2 \rangle / \langle k \rangle = 37.91$ (Table 4.1). Inserting this ratio into (8.7) we obtain $f_c = 0.972$. Therefore, we need to remove 97% of the routers to fragment the Internet into disconnected components. The probability that by chance 186,861 routers fail simultaneously, representing 97% of the $N = 192{,}244$ routers on the Internet, is effectively zero. This is the reason why the topology of the Internet is so robust to random failures.

In general a network displays *enhanced robustness* if its breakdown threshold deviates from the random network prediction (8.8), i.e. if

$$f_c > f_c^{ER}. \tag{8.11}$$

Enhanced robustness has several ramifications:

- The inequality (8.11) is satisfied for most networks for which $\langle k^2 \rangle$ deviates from $\langle k \rangle (\langle k \rangle + 1)$. According to Figure 4.8, for virtually all reference networks $\langle k^2 \rangle$ exceeds the random expectation. Hence the robustness predicted by (8.7) affects most networks of practical interest. This is illustrated in Table 8.1, that shows that for most reference networks (8.11) holds.

- Equation (8.7) predicts that the degree distribution of a network does not need to follow a strict power law to display enhanced robustness. All we need is a larger $\langle k^2 \rangle$ than expected for a random network of similar size.

- The scale-free property changes not only f_c, but also the critical exponents γ_p, β_p and ν in the vicinity of f_c. Their dependence on the degree exponent γ is discussed in ADVANCED TOPICS 8.A.

- Enhanced robustness is not limited to node removal, but emerges under link removal as well (Figure 8.10).

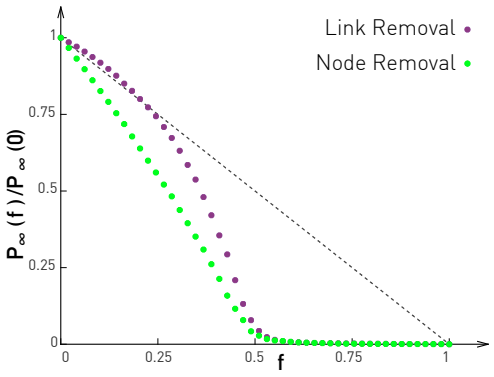


Figure 8.10
Robustness and Link Removal

What happens if we randomly remove the links rather than the nodes? The calculations predict that the critical threshold f_c is the same for random link and node removal [7, 8]. To illustrate this, we compare the impact of random node and link removal on a random network with $\langle k \rangle = 2$. The plot indicates that the network falls apart at the same critical threshold $f_c \approx 0.5$. The difference is in the shape of the two curves. Indeed, the removal of an f fraction of nodes leaves us with a smaller giant component than the removal of an f fraction of links. This is not unexpected: on average each node removes $\langle k \rangle$ links. Hence the removal of an f fraction of nodes is equivalent with the removal of an $f\langle k \rangle$ fraction of links, which clearly makes more damage than the removal of an f fraction of links.

In summary, in this section we encountered a fundamental property of real networks: their robustness to random failures. Equation (8.7) predicts that the breakdown threshold of a network depends on $\langle k \rangle$ and $\langle k^2 \rangle$, which in turn are uniquely determined by the network's degree distribution. Therefore random networks have a finite threshold, but for scale-free networks with $\gamma < 3$ the breakdown threshold converges to one. In other words, we need to remove all nodes to break a scale-free network apart, indicating that these networks show an extreme robustness to random failures.

The origin of this extreme robustness is the large $\langle k^2 \rangle$ term. Given that for most real networks $\langle k^2 \rangle$ is larger than the random expectation, enhanced robustness is a generic property of many networks. This robustness is rooted in the fact that random failures affect mainly the numerous small nodes, which play only a limited role in maintaning a network's integrity.

NETWORK	RANDOM FAILURES (REAL NETWORK)	RANDOM FAILURES (RANDOMIZED NETWORK)	ATTACK (REAL NETWORK)
Internet	0.92	0.84	0.16
WWW	0.88	0.85	0.12
Power Grid	0.61	0.63	0.20
Mobile-Phone Call	0.78	0.68	0.20
Email	0.92	0.69	0.04
Science Collaboration	0.92	0.88	0.27
Actor Network	0.98	0.99	0.55
Citation Network	0.96	0.95	0.76
E. Coli Metabolism	0.96	0.90	0.49
Yeast Protein Interactions	0.88	0.66	0.06

Table 8.1

Breakdown Thresholds Under Random Failures and Attacks

The table shows the estimated f_c for random node failures (second column) and attacks (fourth column) for ten reference networks. The procedure for determining f_c is described in ADVANCED TOPICS 8.E. The third column (randomized network) offers f_c for a network whose N and L coincides with the original network, but whose nodes are connected randomly to each other (randomized network, f_c^{ER}, determined by (8.8)). For most networks f_c for random failures exceeds f_c^{ER} for the corresponding randomized network, indicating that these networks display enhanced robustness, as they satisfy (8.11). Three networks lack this property: the power grid, a consequence of the fact that its degree distribution is exponential (Figure 8.31a), and the actor and the citation networks, which have a very high $\langle k \rangle$, diminishing the role of the high $\langle k^2 \rangle$ in (8.7).

ATTACK TOLERANCE

The important role the hubs play in holding together a scale-free network motivates our next question: What if we do not remove the nodes randomly, but go after the hubs? That is, we first remove the highest degree node, followed by the node with the next highest degree and so on. The likelihood that nodes would break in this particular order under normal conditions is essentially zero. Instead this process mimics an *attack* on the network, as it assumes a detailed knowledge of the network topology, an ability to target the hubs, and a desire to deliberately cripple the network [1].

The removal of a single hub is unlikely to fragment a network, as the remaining hubs can still hold the network together. After the removal of a few hubs, however, large chunks of nodes start falling off (Online Resource 8.2). If the attack continues, it can rapidly break the network into tiny clusters.

The impact of hub removal is quite evident in the case of a scale-free network (Figure 8.11): the critical point, which is absent under random failures, reemerges under attacks. Not only reemerges, but it has a remarkably low value. Therefore the removal of a small fraction of the hubs is sufficient to break a scale-free network into tiny clusters. The goal of this section is to quantify this attack vulnerability.

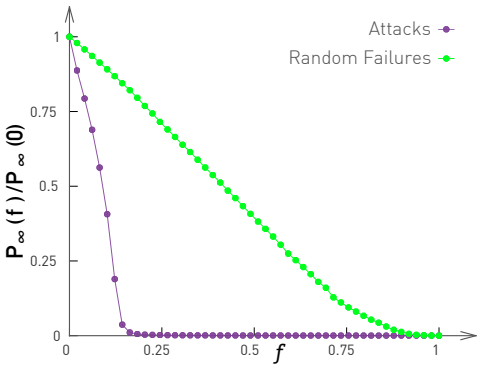


Figure 8.11
Scale-free Network Under Attack

The probability that a node belongs to the largest connected component in a scale-free network under attack (purple) and under random failures (green). For an attack we remove the nodes in a decreasing order of their degree: we start with the biggest hub, followed by the next biggest and so on. In the case of failures the order in which we choose the nodes is random, independent of the node's degree. The plot illustrates a scale-free network's extreme fragility to attacks: f_c is small, implying that the removal of only a few hubs can disintegrate the network. The initial network has degree exponent $\gamma = 2.5$, $k_{min} = 2$ and $N = 10{,}000$.

Critical Threshold Under Attack

An attack on a scale-free network has two consequences (Figure 8.11):

- The critical threshold f_c is smaller than $f_c = 1$, indicating that under attacks a scale-free network can be fragmented by the removal of a finite fraction of its hubs.

- The observed f_c is remarkably low, indicating that we need to remove only a tiny fraction of the hubs to cripple the network.

To quantify this process we need to analytically calculate f_c for a net-

work under attack. To do this we rely on the fact that hub removal changes the network in two ways [9]:

- It changes the maximum degree of the network from k_{max} to k'_{max} as all nodes with degree larger than k'_{max} have been removed.

- The degree distribution of the network changes from p_k to $p'_{k'}$, as nodes connected to the removed hubs will loose links, altering the degrees of the remaining nodes.

By combining these two changes we can map the attack problem into the robustness problem discussed in the previous section. In other words, we can view an attack as random node removal from a network with adjusted k'_{max} and $p'_{k'}$. The calculations predict that the critical threshold f_c for attacks on a scale-free network is the solution of the equation [9, 10] (ADVANCED TOPICS 8.F)

$$f_c^{\frac{2-\gamma}{1-\gamma}} = 2 + \frac{2-\gamma}{3-\gamma} k_{min} (f_c^{\frac{3-\gamma}{1-\gamma}} - 1). \qquad (8.12)$$

Figure 8.12 shows the numerical solution of (8.12) in function of the degree exponent γ, allowing us to draw several conclusions:

- While f_c for failures decreases monotonically with γ, f_c for attacks can have a non-monotonic behavior: it increases for small γ and decreases for large γ.

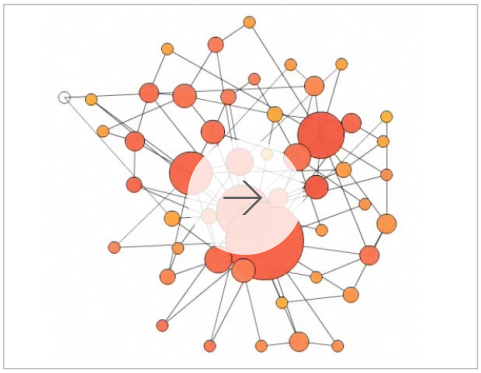
- f_c for attacks is always smaller than f_c for random failures.

- For large γ a scale-free network behaves like a random network. As a random network lacks hubs, the impact of an attack is similar to the impact of random node removal. Consequently the failure and the attack thresholds converge to each other for large γ. Indeed, if $\gamma \to \infty$ then $p_k \to \delta(k - k_{min})$, meaning that all nodes have the same degree k_{min}. Therefore random failures and targeted attacks become indistinguishable in the $\gamma \to \infty$ limit, obtaining

$$f_c \to 1 - \frac{1}{(k_{min} - 1)} \qquad (8.13)$$

- As Figure 8.13 shows, a random network has a finite percolation threshold under both random failures and attacks, as predicted by Figure 8.12 and (8.13) for large γ.

The airport analogy helps us understand the fragility of scale-free networks to attacks: The closing of two large airports, like Chicago's O'Hare Airport or the Atlanta International Airport, for only a few hours would be headline news, altering travel throughout the U.S. Should some series of events lead to the simultaneous closure of the Atlanta, Chicago, Denver, and New York airports, the biggest hubs, air travel within the North American continent would come to a halt within hours.



Online Resource 8.2

Scale-free Networks Under Attack

During an attack we aim to inflict maximum damage on a network. We can do this by removing first the highest degree node, followed by the next highest degree, and so on. As the movie illustrates, it is sufficient to remove only a few hubs to break a scale-free network into disconnected components. Compare this with the network's refusal to break apart under random node failures, shown in Online Resource 8.1. Visualization by Dashun Wang.

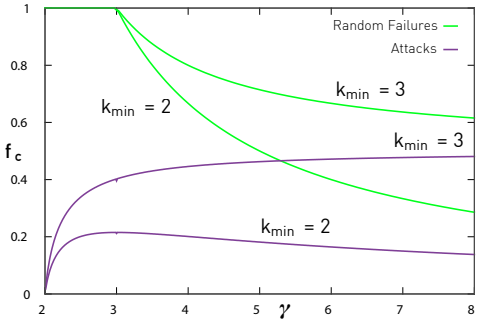


Figure 8.12

Critical Threshold Under Attack

The dependence of the breakdown threshold, f_c, on the degree exponent γ for scale-free networks with $k_{min} = 2, 3$. The curves are predicted by (8.12) for attacks (purple) and by (8.7) for random failures (green).

In summary, while random node failures do not fragment a scale-free network, an attack that targets the hubs can easily destroy such a network. This fragility is bad news for the Internet, as it indicates that it is inherently vulnerable to deliberate attacks. It can be good news in medicine, as the vulnerability of bacteria to the removal of their hub proteins offers avenues to design drugs that kill unwanted bacteria.

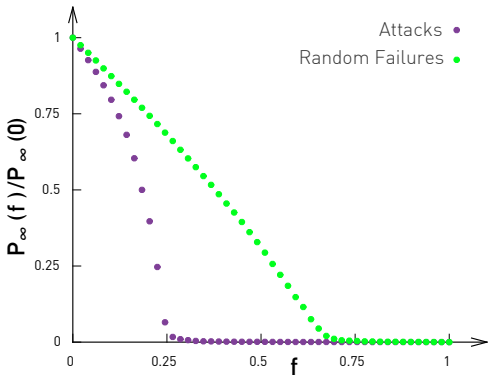


Figure 8.13

Attacks and Failures in Random Networks

The fraction of nodes that belong to the giant component in a random network if an f fraction of nodes are randomly removed (green) and in decreasing order of their degree (purple). Both curves indicate the existence of a finite threshold, in contrast with scale-free networks, for which $f_c \to 1$ under random failures. The simulations were performed for random networks with $N = 10{,}000$ and $\langle k \rangle = 3$.

BOX 8.2

PAUL BARAN AND THE INTERNET

In 1959 RAND, a Californian think-tank, has assigned Paul Baran, a young engineer at that time, to develop a communication system that can survive a Soviet nuclear attack. As a nuclear strike handicaps all equipment within the range of the detonation, Baran had to design a system whose users outside this range do not loose contact with one another. He described the communication network of his time as a "hierarchical structure of a set of stars connected in the form of a larger star," offering an early description of what we call today a scale-free network [11]. He concluded that this topology is too centralized to be viable under attack. He also discarded the hub-and-spoke topology shown in Figure 8.14a, noting that the "centralized network is obviously vulnerable as destruction of a single central node destroys communication between the end stations."

Baran decided that the ideal survivable architecture was a distributed mesh-like network (Figure 8.14c). This network is sufficiently redundant, so that even if some of its nodes fail, alternative paths can connect the remaining nodes. Baran's ideas were ignored by the military, so when the Internet was born a decade later, it relied on distributed protocols that allowed each node to decide where to link. This decentralized philosophy paved the way to the emergence of a scale-free Internet, rather than the uniform mesh-like topology envisioned by Baran.

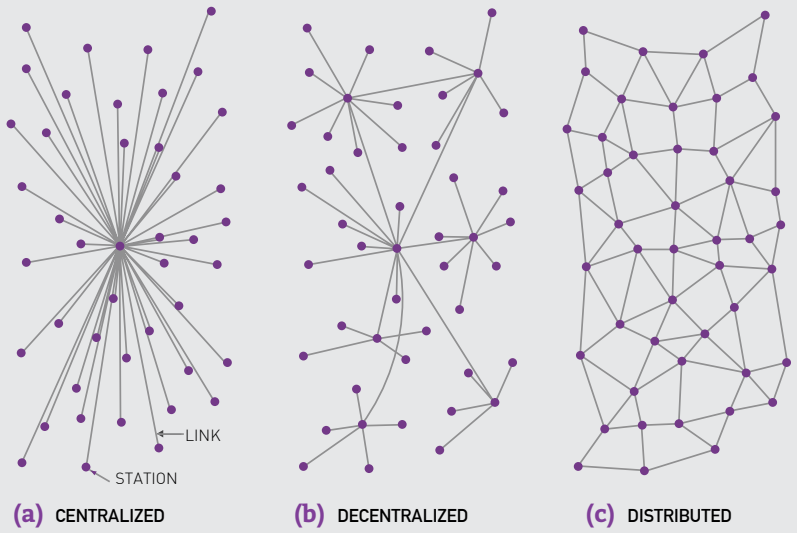


Figure 8.14
Baran's Network

Possible configurations of communication networks, as envisioned by Paul Baran in 1959. After [11].

CASCADING FAILURES

Throughout this chapter we assumed that each node failure is a random event, hence the nodes of a network fail independently of each other. In reality, in a network the activity of each node depends on the activity of its neighboring nodes. Consequently the failure of a node can induce the failure of the nodes connected to it. Let us consider a few examples:

- **Blackouts (Power Grid)**
  After the failure of a node or a link the electric currents are instantaneously reorganized on the rest of the power grid. For example, on August 10, 1996, a hot day in Oregon, a line carrying 1,300 megawatts sagged close to a tree and snapped. Because electricity cannot be stored, the current it carried was automatically shifted to two lower voltage lines. As these were not designed to carry the excess current, they too failed. Seconds later the excess current lead to the malfunction of thirteen generators, eventually causing a blackout in eleven U.S. states and two Canadian provinces [12].

- **Denial of Service Attacks (Internet)**
  If a router fails to transmit the packets received by it, the Internet protocols will alert the neighboring routers to avoid the troubled equipment by re-routing the packets using alternative routes. Consequently a failed router increases traffic on other routers, potentially inducing a series of denial of service attacks throughout the Internet [13].

- **Financial Crises**
  Cascading failures are common in economic systems. For example, the drop in the house prices in 2008 in the U.S. has spread along the links of the financial network, inducing a cascade of failed banks, companies and even nations [14, 15, 16]. It eventually caused the worst global financial meltdown since the 1930s Great Depression.

While they cover different domains, these examples have several common characteristics. First, the initial failure had only limited impact on

Figure 8.15
Domino Effect

The *domino effect* is the fall of a series of dominos induced by the fall of the first domino. The term is often used to refer to a sequence of events induced by a local change, that propagates through the whole system. Hence the domino effect represents perhaps the simplest illustration of cascading failures, the topic of this section.

the network structure. Second, the initial failure did not stay localized, but it spread along the links of the network, inducing additional failures. Eventually, multiple nodes lost their ability to carry out their normal functions. Consequently each of these systems experienced *cascading failures*, a dangerous phenomena in most networks [17]. In this section we discuss the empirical patterns governing such cascading failures. The modeling of these events is the topic of the next section.

EMPIRICAL RESULTS

Cascading failures are well documented in the case of the power grid, information systems and tectonic motion, offering detailed statistics about their frequency and magnitude.

- **Blackouts**

  A blackout can be caused by power station failures, damage to electric transmission lines, a short circuit, and so on. When the operating limits of a component is exceeded, it is automatically disconnected to protect it. Such failure redistributes the power previously carried by the failed component to other components, altering the power flow, the frequency, the voltage and the phase of the current, and the operation of the control, monitoring and alarm systems. These changes can in turn disconnect other components as well, starting an avalanche of failures.

  A frequently recorded measure of blackout size is the energy unserved. Figure 8.17a shows the probability distribution $p(s)$ of energy unserved in all North American blackouts between 1984 and 1998. Electrical engineers approximate the obtained distribution with the power law [18],

$$p(s) \sim s^{-\alpha}, \tag{8.14}$$

  where the *avalanche exponent* α is listed in Table 8. 2 for several countries. The power law nature of this distribution indicates that most blackouts are rather small, affecting only a few consumers. These coexists, however, with occasional major blackouts, when millions of consumers lose power (Figure 8.16).

- **Information Cascades**

  Modern communication systems, from email to Facebook or Twitter, facilitate the cascade-like spreading of information along the links of the social network. As the events pertaining to the spreading process often leave digital traces, these platforms allow researchers to detect the underlying cascades.

  The micro-blogging service Twitter has been particularly studied in this context. On Twitter the network of who follows whom can be reconstructed by crawling the service's follower graph. As users frequently share web-content using URL shorteners, one can also track each spreading/sharing process. A study tracking 74 million such events over two months followed the diffusion of each URL from a

Figure 8.16

Northeast Blackout of 2003

One of the largest blackouts in North America took place on August 14, 2003, just before 4:10 p.m. Its cause was a software bug in the alarm system at a control room of the *First Energy Corporation* in Ohio. Missing the alarm, the operators were unaware of the need to redistribute the power after an overloaded transmission line hit a tree. Consequently a normally manageable local failure began a cascading failure that shut down more than 508 generating units at 265 power plants, leaving an estimated 10 million people without electricity in Ontario and 45 million in eight U.S. states. The figure highlights the states affected by the August 14, 2003 blackout. For a satelite image of the blackout, see Figure 1.1.

particular seed node through its reposts until the end of a cascade (Figure 8.18). As Figure 8.17b indicates, the size distribution of the observed cascades follows the power-law (8.14) with an avalanche exponent $\alpha \approx 1.75$ [19]. The power law indicates that the vast majority of posted URLs do not spread at all, a conclusion supported by the fact that the average cascade size is only $\langle s \rangle = 1.14$. Yet, a small fraction of URLs are reposted thousands of times.

- **Earthquakes**

  Geological fault surfaces are irregular and sticky, prohibiting their smooth slide against each other. Once a fault has locked, the continued relative motion of the tectonic plates accumulate an increasing amount of strain energy around the fault surface. When the stress becomes sufficient to break through the asperity, a sudden slide releases the stored energy, causing an earthquake. Earthquakes can be also induced by the natural rupture of geological faults, by volcanic activity, landslides, mine blasts and even nuclear tests.

  Each year around 500,000 earthquakes are detected with instrumentation. Only about 100,000 of these are sufficiently strong to be felt by humans. Seismologists approximate the distribution of earthquake amplitudes with the power law (8.14) with $\alpha \approx 1.67$ (Figure 8.17c) [20].

  Earthquakes are rarely considered a manifestly network phenomenon, given the difficulty of mapping out the precise network of interdependencies that causes them. Yet, the resulting cascading failures bear many similarities to network-based cascading events, suggesting common mechanisms.

  The power-law distribution (8.14) followed by blackouts, information cascades and earthquakes indicates that most cascading failures are relatively small. These small cascades capture the loss of electricity in a few houses, tweets of little interest to most users, or earthquakes so small that one needs sensitive instruments to detect them. Equation (8.14) predicts that these numerous small events coexist with a few exceptionally large events. Examples of such major cascades include the 2003 power outage in North America (Figure 8.16), the tweet *Iran Election Crisis: 10 Incredible YouTube Videos http://bit.ly/vPDLo* that was shared 1,399 times [21], or the January 2010 earthquake in Haiti, with over 200,000 victims. Interestingly, the avalanche exponents reported by electrical engineers, media researches and seismologists are surprisingly close to each other, being between 1.6 and 2 (Table 8.2).

  Cascading failures are documented in many other environments:

  - The consequences of bad weather or mechanical failures can cascade through airline schedules, delaying multiple flights and

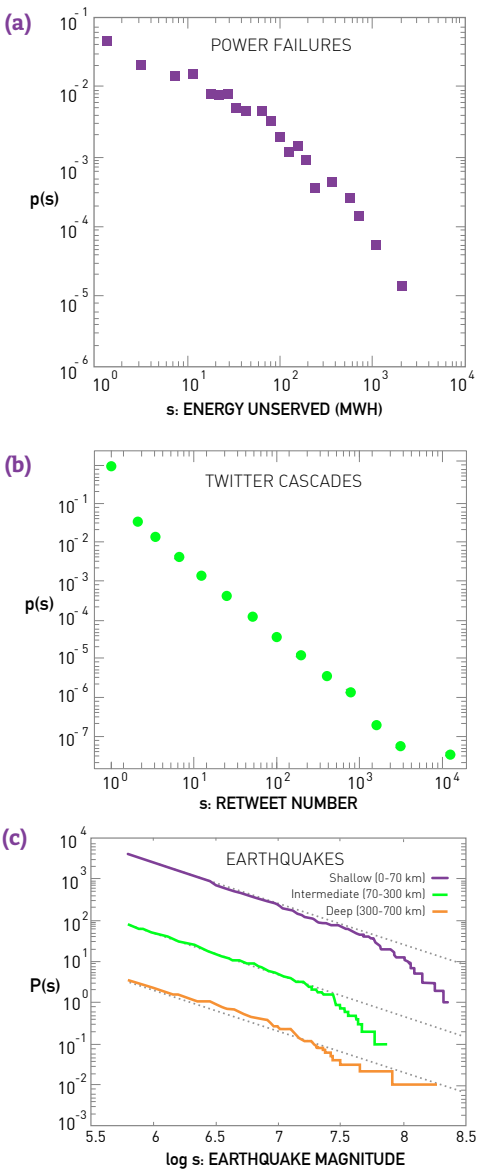


Figure 8.17
Cascade Size Distributions

(a) The distribution of energy loss for all North American blackouts between 1984 and 1998, as documented by the North American Electrical Reliability Council. The distribution is typically fitted to **(8.14)**. The reported exponents for different countries are listed in **Table 8.2**. After [18].

(b) The distribution of cascade sizes on Twitter. While most tweets go unnoticed, a tiny fraction of tweets are shared thousands of times. Overall the retweet numbers are well approximated with **(8.14)** with $\alpha \simeq 1.75$. After [19].

(c) The cumulative distribution of earthquake amplitudes recorded between 1977 and 2000. The dashed lines indicate the power law fit **(8.14)** used by seismologists to characterize the distribution. The earthquake magnitude shown on the horizontal axis is the logarithm of s, which is the amplitude of the observed seismic waves. After [20].

stranding thousands of passengers (BOX 8.3) [22].

- The disappearance of a species can cascade through the food web of an ecosystem, inducing the extinction of numerous species and altering the habitat of others [23, 24, 25, 26].

- The shortage of a particular component can cripple supply chains. For example, the 2011 floods in Thailand have resulted in a chronic shortage of car components that disrupted the production chain of more than 1,000 automotive factories worldwide. Therefore the damage was not limited to the flooded factories, but resulted in worldwide insurance claims reaching $20 billion [27].

In summary, cascading effects are observed in systems of rather different nature. Their size distribution is well approximated with the power law (8.14), implying that most cascades are too small to be noticed; a few, however, are huge, having a global impact. The goal of the next section is to understand the origin of these phenomena and to build models that can reproduce its salient features.

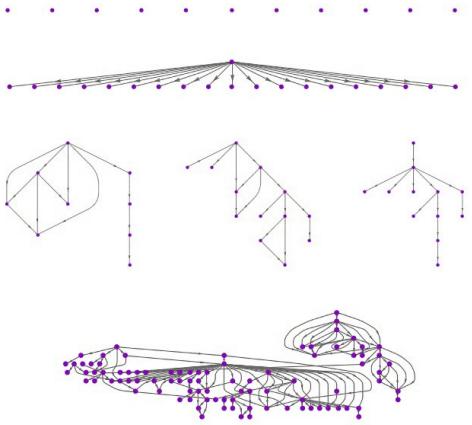


Figure 8.18
Information Cascades

Examples of information cascades on Twitter. Nodes denote Twitter accounts, the top node corresponding to the account that first posted a certain shortened URL. The links correspond to those who retweeted it. These cascades capture the heterogeneity of information avalanches: most URLs are not retweeted at all, appearing as single nodes in the figure. Some, however, start major retweet avalanches, like the one seen at the bottom panel. After [19].

SOURCE	EXPONENT	CASCADE
Power grid (North America)	2.0	Power
Power grid (Sweden)	1.6	Energy
Power grid (Norway)	1.7	Power
Power grid (New Zealand)	1.6	Energy
Power grid (China)	1.8	Energy
Twitter Cascades	1.75	Retweets
Earthquakes	1.67	Seismic Wave

Table 8.2
Avalanche Exponents in Real Systems.

The reported avalanche exponents of the power law distribution (8.14) for energy loss in various countries [18], twitter cascades [19] and earthquake sizes [20]. The third column indicates the nature of the measured cascade size s, corresponding to power or energy not served, the number of retweets generated by a typical tweet and the amplitude of the seismic wave.

BOX 8.3

CASCADING FLIGHT CONGESTIONS

Flight delays in the U.S. have an economic impact of over $40 billion per year [28], caused by the need for enhanced operations, passenger loss of time, decreased productivity and missed business and leisure opportunities. A flight delay is the time difference between the expected and actual departure/arrival times of a flight. Airline schedules include a buffer period between consecutive flights to accommodate short delays. When a delay exceeds this buffer, subsequent flights that use the same aircraft, crew or gate, are also delayed. Consequently a delay can propagate in a cascade-like fashion through the airline network.

While most flights in 2010 were on time, 37.5% arrived or departed late [22]. The delay distribution follows (8.14), implying that while most flights were delayed by just a few minutes, a few were hours behind schedule. These long delays induce correlated delay patterns, a signature of cascading congestions in the air transportation system (Figure 8.19).

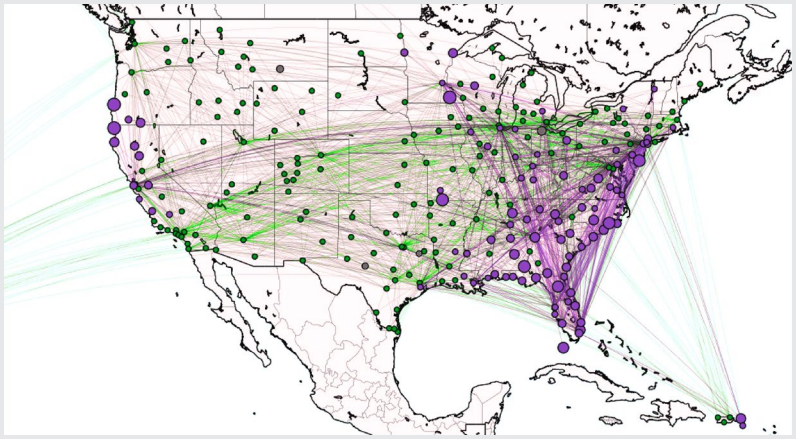


Figure 8.19
Clusters of Congested Airports

U.S. aviation map showing congested airports as purple nodes, while those with normal traffic as green nodes. The lines correspond to the direct flights between them on March 12, 2010. The clustering of the congested airports indicate that the dealys are not independent of each other, but cascade through the airport network. After [22].

MODELING CASCADING FAILURES

The emergence of a cascading event depends on many variables, from the structure of the network on which the cascade propagates, to the nature of the propagation process and the breakdown criteria of each individual component. The empirical results indicate that despite the diversity of these variables, the size distribution of the observed avalanches is universal, being independent of the particularities of the system. The purpose of this section is to understand the mechanisms governing cascading phenomena and to explain the power-law nature of the avalanche size distribution.

Numerous models have been proposed to capture the dynamics of cascading events [18, 29, 30, 31, 32, 33, 34, 35]. While these models differ in the degree of fidelity they employ to capture specific phenomena, they indicate that systems that develop cascades share three key ingredients:

(i) The system is characterized by some flow over a network, like the flow of electric current in the power grid or the flow of information in communication systems.

(ii) Each component has a local breakdown rule that determines when it contributes to a cascade, either by failing (power grid, earthquakes) or by choosing to pass on a piece of information (Twitter).

(iii) Each system has a mechanism to redistribute the traffic to other nodes upon the failure or the activation of a component.

Next, we discuss two models that predict the characteristics of cascading failures at different levels of abstraction.

FAILURE PROPAGATION MODEL

Introduced to model the spread of ideas and opinions [30], the failure propagation model is frequently used to describe cascading failures as well [35]. The model is defined as follows:

Consider a network with an arbitrary degree distribution, where each node contains an agent. An agent i can be in the state *0* (*active* or *healthy*) or 1 (*inactive* or *failed*), and is characterized by a breakdown threshold $\varphi_i = \varphi$ for all i.

All agents are initially in the healthy state 0. At time $t = 0$ one agent switches to state 1, corresponding to an initial component failure or to the release of a new piece of information. In each subsequent time step we randomly pick an agent and update its state following a threshold rule:

- If the selected agent i is in state 0, it inspects the state of its k_i neighbors. The agent i adopts state *1* (i.e. it also fails) if at least a φ fraction of its k_i neighbors are in state *1*, otherwise it retains its original state 0.

- If the selected agent i is in state *1*, it does not change its state.

In other words, a healthy node i changes its state if a φ fraction of its neighbors have failed. Depending on the local network topology, an initial perturbation can die out immediately, failing to induce the failure of any other node. It can also lead to the failure of multiple nodes, as illustrated in Figure 8.20a,b. The simulations document three regimes with distinct avalanche characteristics (Figure 8.20c):

- **Subcritical Regime**
  If $\langle k \rangle$ is high, changing the state of a node is unlikely to move other nodes over their threshold, as the healthy nodes have many healthy neighbors. In this regime cascades die out quickly and their sizes follow an exponential distribution. Hence the system is unable to support large global cascades (blue symbols, Figure 8.20c,d).

- **Supercritical Regime**
  If $\langle k \rangle$ is small, flipping a single node can put several of its neighbors over the threshold, triggering a global cascade. In this regime perturbations induce major breakdowns (purple symbols, Figure 8.20c,d).

- **Critical Regime**
  At the boundary of the subcritical and supercritical regime the avalanches have widely different sizes. Numerical simulations indicate that in this regime the avalanche sizes s follow (8.14) (green and orange symbols, Figure 8.21d) with $\alpha = 3/2$ if the underlying network is random.

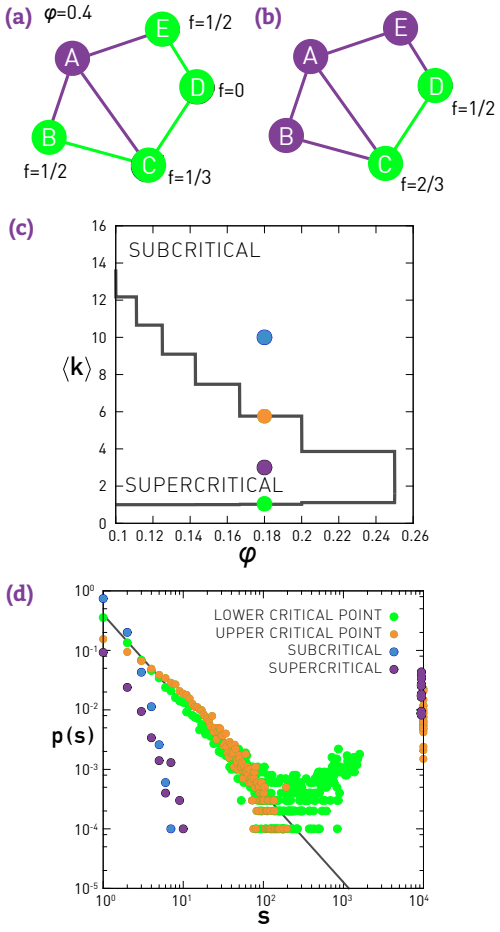


Figure 8.20
Failure Propagation Model

(a,b) The development of a cascade in a small network in which each node has the same breakdown threshold $\varphi = 0.4$. Initially all nodes are in state 0, shown as green circles. After node A changes its state to 1 (purple), its neighbors *B* and *E* will have a fraction $f = 1/2 > 0.4$ of their neighbors in state 1. Consequently they also fail, changing their state to 1, as shown in (b). In the next time step *C* and *D* will also fail, as both have $f > 0.4$. Consequently the cascade sweeps the whole network, reaching a size $s = 5$. One can check that if we initially flip node *B*, it will not induce an avalanche.

(c) The phase diagram of the failure propagation model in terms of the threshold function φ and the average degree $\langle k \rangle$ of the network on which the avalanche propagates. The continuous line encloses the region of the $(\langle k \rangle, \varphi)$ plane in which the cascades can propagate in a random graph.

(d) Cascade size distributions for $N = 10{,}000$ and $\varphi = 0.18$, $\langle k \rangle = 1.05$ (green), $\langle k \rangle = 3.0$ (purple), $\langle k \rangle = 5.76$ (orange) and $\langle k \rangle = 10.0$ (blue). At the lower critical point we observe a power law $p(s)$ with exponent $\alpha = 3/2$. In the supercritical regime we have only a few small avalanches, as most cascades are global. In the upper critical and subcritical regime we see only small avalanches. After [30].

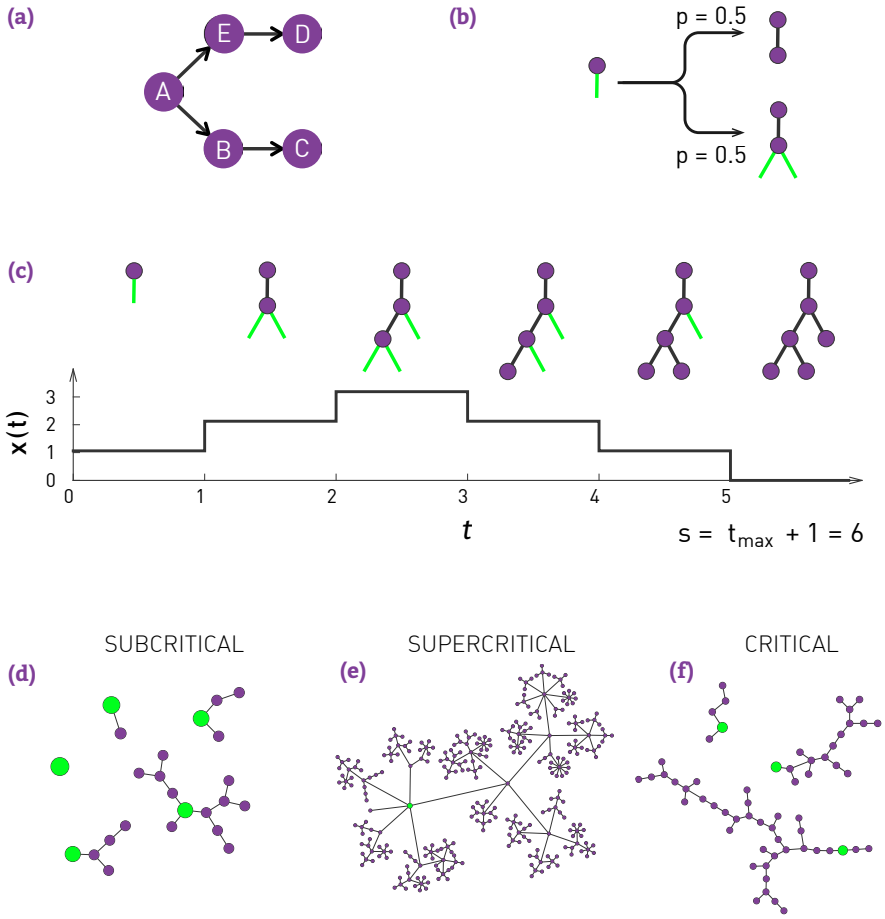


Figure 8.21
Branching Model

(a) The branching process mirroring the propagation of the failure shown in Figure 8.20a,b. The perturbation starts from node *A*, whose failure flips *B* and *E*, which in turn flip *C* and *D*, respectively.

(b) An elementary branching process. Each active link (green) can become inactive with probability $p_0 = 1/2$ (top) or give birth to two new active links with probability $p_2 = 1/2$ (bottom).

(c) To analytically calculate *p(s)* we map the branching process into a diffusion problem. For this we show the number of active sites, *x(t)*, in function of time *t*. A nonzero *x(t)* means that the avalanche persists. When *x(t)* becomes zero, we loose all active sites and the avalanche ends. In the example shown in the image this happens at $t = 5$, hence the size of the avalanche is $t_{max} + 1 = 6$.

An exact mapping between the branching model and a one dimensional random walk helps us calculate the avalanche exponent. Consider a branching process starting from a stub with one active end. When the active site becomes inactive, it decreases the number of its active sites, i.e. $x \to x - 1$. When the active site branches, creates two active sites, i.e. $x \to x + 1$. This maps the avalanche size *s* to the time it takes for the walk that starts at $x = 1$ to reach $x = 0$ for the first time. This is a much studied process in random walk theory, predicting that the return time distribution follows a power law with exponent 3/2 [32]. For branching process corresponding to scale-free p_k, the avalanche exponent depends on γ, as shown in Figure 8.22.

(d,e,f) Typical avalanches generated by the branching model in the subcritical **(d)**, supercritical **(e)** and critical regime **(f)**. The green node in each cascade marks the root of the tree, representing the first perturbation. In **(d)** and **(f)** we show multiple trees, while in **(e)** we show only one, as each tree (avalanche) grows indefinitely.

BRANCHING MODEL

Given the complexity of the failure propogation model, it is hard to analytically predict the scaling behavior of the obtained avalanches. To understand the power-law nature of *p(s)* and to calculate the avalanche exponent *α*, we turn to the branching model. This is the simplest model that still captures the basic features of a cascading event.

The model builds on the observation that each cascading failure follows a branching process. Indeed, let us call the node whose initial failure triggers the avalanche the *root of the tree*. The branches of the tree are the nodes whose failure was triggered by this initial failure. For example, in Figures 8.20a,b, the breakdown of node *A* starts the avalanche, hence *A* is the root of the tree. The failure of *A* leads to the failure of *B* and *E*, representing the two branches of the tree. Subsequently *E* induces the failure of *D* and *B* leads to the failure of *C* (Figure 8.21a).

The branching model captures the essential features of avalanche propagation (Figure 8.21). The model starts with a single active node. In the next time step each active node produces *k* offsprings, where *k* is selected from a p_k distribution. If a node selects $k = 0$, that branch dies out (Figure 8.21b). If it selects $k > 0$, it will have *k* new active sites. The size of an avalanche corresponds to the size of the tree when all active sites died out (Figure 8.21c).

The branching model predicts the same phases as those observed in the cascading failures model. The phases are now determined only by $\langle k \rangle$, hence by the p_k distribution:

- **Subcritical Regime:** $\langle k \rangle < 1$
  For $\langle k \rangle < 1$ on average each branch has less then one offspring. Consequently each tree will terminate quickly (Figure 8.21d). In this regime the avalanche sizes follow an exponential distribution.

- **Supercritical Regime:** $\langle k \rangle > 1$
  For $\langle k \rangle > 1$ on average each branch has more than one offspring. Consequently the tree will continue to grow indefinitely (Figure 8.21e). Hence in this regime all avalanches are global.

- **Critical Regime:** $\langle k \rangle = 1$
  For $\langle k \rangle = 1$ on average each branch has exactly one offspring. Consequently some trees are large and others die out shortly (Figure 8.21e). Numerical simulations indicate that in this regime the avalanche size distribution follows the power law (8.14).

The branching model can be solved analytically, allowing us to determine the avalanche size distribution for an arbitrary p_k. If p_k is exponentially bounded, *e.g.* it has an exponential tail, the calculations predict $\alpha = 3/2$. If, however, p_k is scale-free, then the avalanche exponent depends on the power-law exponent γ, following (Figure 8.22) [32, 33]

$$\alpha = \begin{cases} 3/2, & \gamma \geq 3 \\ \gamma/(\gamma-1), & 2 < \gamma < 3 \end{cases}. \qquad (8.15)$$

This prediction allows us to revisit Table 8.2, finding that the empirically observed avalanche exponents are all between 1.5 and 2, as predicted by (8.15).

In summary, we discussed two models that capture the dynamics of cascading failures: the failure propagation model and the branching model. In the literature we may also encounter the *overload model*, which is designed to capture power grid failures [18], or the *sandpile model*, that captures the behavior of cascading failures in the critical regime [31, 32]. Other models can also account for the fact that nodes and links have different capacities to carry traffic [34]. These models differ in their realism and the number and the nature of their tuning parameters. Yet, they all predict the existence of a critical state, in which the avalanche sizes follow a power law. The avalanche exponent α is uniquely determined by the degree exponent of the network on which the avalanche propagates. The fact that models with rather different propagation dynamics and failure mechanisms predict the same scaling law and avalanche exponent suggests that the underlying phenomena is universal, i.e. it is model independent.

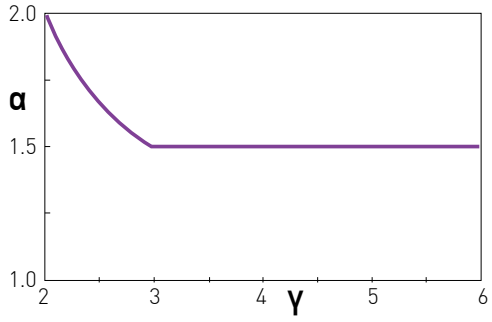


Figure 8.22
The Avalanche Exponent

The dependence of the avalanche exponent α on the degree exponent γ of the network on which the avalanche propagates, according to (8.15). The plot indicates that between $2 < \gamma < 3$ the avalanche exponent depends on the degree exponent. Beyond $\gamma = 3$, however, the avalanches behave as they would be spreading on a random network, in which case we have $\alpha = 3/2$.

BUILDING ROBUSTNESS

Can we enhance a network's robustness? In this section we show that the insights we gained about the factors that influence robustness allows us to design networks that can simultaneously resist random failures and attacks. We also discuss how to stop a cascading failure, allowing us to enhance a system's dynamical robustness. Finally, we apply the developed tools to the power grid, linking its robustness to its reliability.

Designing Robust Networks

Designing networks that are simultaneously robust to attacks *and* random failures appears to be a conflicting desire [36, 37, 38, 39]. For example, the hub-and-spoke network of Figure 8.23a is robust to random failures, as only the failure of its central node can break the network into isolated components. Therefore, the probability that a random failure will fragment the network is $1/N$, which is negligible for large N. At the same time this network is vulnerable to attacks, as the removal of a single node, its central hub, breaks the network into isolated nodes.

We can enhance this network's attack tolerance by connecting its peripheral nodes (Figure 8.23b), so that the removal of the hub does not fragment the network. There is a price, however, for this enhanced robustness: it requires us to double the number of links. If we define the cost to build and maintain a network to be proportional to its average degree $\langle k \rangle$, the cost of the network of Figure 8.23b is 24/7, double of the cost 12/7 of the network of Figure 8.23a. The increased cost prompts us to refine our question: Can we maximize the robustness of a network to both random failures and targeted attacks without changing the cost?

A network's robustness against random failures is captured by its percolation threshold f_c, which is the fraction of the nodes we must remove for the network to fall apart. To enhance a network's robustness we must increase f_c. According to (8.7) f_c depends only on $\langle k \rangle$ and $\langle k^2 \rangle$. Consequently the degree distribution which maximizes f_c needs to maximize $\langle k^2 \rangle$ if we wish to keep the cost $\langle k \rangle$ fixed. This is achieved by a bimodal distribution, corresponding to a network with only two kinds

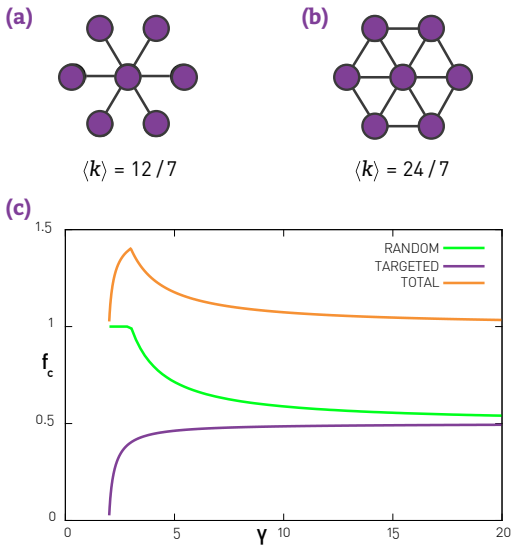


Figure 8.23
Enhancing Robustness

(a) A hub-and-spoke network is robust to random failures but has a low tolerance to an attack that removes its central hub.

(b) By connecting some of the small degree nodes, the reinforced network has a higher tolerance to targeted attacks. This increases the cost measured by $\langle k \rangle$, which is higher for the reinforced network.

(c) Random, f_c^{rand}, targeted f_c^{targ} and total f_c^{tot} percolation thresholds for scale-free networks in function of the degree exponent γ for a network with $k_{min} = 3$.

of nodes, with degrees k_{min} and k_{max} (Figure 8.23a,b).

If we wish to simultaneously optimize the network topology against both random failures and attacks, we search for topologies that maximize the sum (Figure 8.24c)

$$f_c^{tot} = f_c^{rand} + f_c^{targ}. \tag{8.16}$$

A combination of analytical arguments and numerical simulations indicate that this too is best achieved by the bimodal degree distribution [36, 37, 38, 39]

$$p_k = (1-r)\delta(k-k_{min}) + r\delta(k-k_{max}), \tag{8.17}$$

describing a network in which an r fraction of nodes have degree k_{max} and the remaining $(1 - r)$ fraction have degree k_{min}.

As we show in ADVANCED TOPICS 8.G, the maximum of f_c^{tot} is obtained when $r = 1/N$, i.e. when there is a single node with degree k_{max} and the remaining nodes have degree k_{min}. In this case the value of k_{max} depends on the system size as

$$k_{max} = AN^{2/3}. \tag{8.18}$$

In other words, a network that is robust to both random failures and attacks has a single hub with degree (8.18), and the rest of the nodes have the same degree k_{min}. This hub-and-spoke topology is obviously robust against random failures as the chance of removing the central hub is $1/N$, tiny for large N.

The obtained network may appear to be vulnerable to an attack that removes its hub, but it is not necessarily so. Indeed, the network's giant component is held together by both the central hub as well as by the many nodes with degree k_{min}, that for $k_{min} > 1$ form a giant component on their own. Hence while the removal of the k_{max} hub causes a major one-time loss, the remaining low degree nodes are robust against subsequent targeted removal (Figure 8.24c).

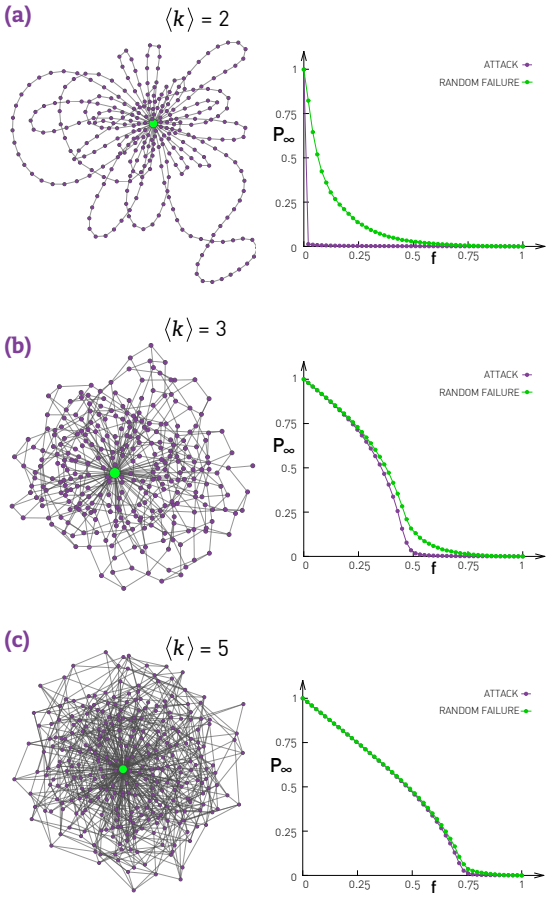


Figure 8.24
Optimizing Attack and Failure Tolerance

The figure illustrates the optimal network topologies predicted by (8.16) and (8.17), consisting of a single hub of size (8.18) and the rest of the nodes have the same degree k_{min} determined by $\langle k \rangle$. The left panels show the network topology for $N = 300$; the right panels show the failure/attack curves for $N = 10{,}000$.

(a) For small $\langle k \rangle$ the hub holds the network together. Once we remove this central hub the network breaks apart. Hence the attack and error curves are well separated, indicating that the network is robust to random failures but fragile to attacks.

(b) For larger $\langle k \rangle$ a giant component emerges, that exists even without the central hub. Hence while the hub enhances the system's robustness to random failures, it is no longer essential for the network. In this case both the attack f_c^{targ} and error f_c^{rand} are large.

(c) For even larger $\langle k \rangle$ the error and the attack curves are indistinguishable, indicating that the network's response to attacks and random failures is indistinguishable. In this case the network is well connected even without its central hub.

BOX 8.4

HALTING CASCADING FAILURES

Can we avoid cascading failures? The first instinct is to reinforce the network by adding new links. The problem with reinforcement is that in most real systems the time needed to establish a new link is much larger than the timescale of a cascading failure. For example, thanks to regulatory, financial and legal barriers, building a new transmission line on the power grid can take up to two decades. In contrast, a cascading failure can sweep the power grid in a few seconds.

In a counterintuitive fashion, the impact of cascading failures can be reduced through selective node and link removal [40]. To do so we note that each cascading failure has two parts:

(i) *Initial failure* is the breakdown of the first node or link, representing the source of the subsequent cascade.

(ii) *Propagation* is when the initial failure induces the failure of additional nodes and starts cascading through the network.

Typically the time interval between (i) and (ii) is much shorter than the time scale over which the network could be reinforced. Yet, simulations indicate that the size of a cascade can be reduced if we intentionally remove additional nodes right after the initial failure (i), but before the failure could propagate. Even though the intentional removal of a node or a link causes further damage to the network, the removal of a well chosen component can suppress the cascade propagation [40]. Simulations indicate that to limit the size of the cascades we must remove nodes with small loads and links with large excess load in the vicinity of the initial failure. The mechanism is similar to the method used by firefighters, who set a controlled fire in the fireline to consume the fuel in the path of a wildfire.

A dramatic manifestation of this approach is provided by the *Lazarus effect*, the ability to revive a previously "dead" bacteria, i.e. one that is unable to grow and multiply. This can be achieved through the knockout of a few well selected genes (Figure 8.25) [41]. Therefore, in a counterintuitive fashion, controlled damage can be beneficial to a network.

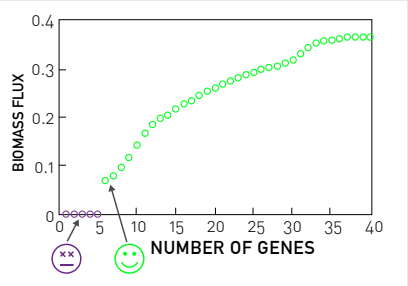


Figure 8.25
Lazarus Effect

The growth rate of a bacteria is determined by its ability to generate biomass, the molecules it needs to build its cell wall, DNA and other cellular components. If some key genes are missing, the bacteria is unable to generate the necessary biomass. Unable to multiply, it will eventually die. Genes in whose absence the *biomass flux* is zero are called *essential*.

The plot shows the biomass flux for E. *Coli*, a bacteria frequently studied by biologists. The original mutant is missing an essential gene, hence its biomass flux is zero, as shown on the vertical axis. Consequently, it cannot multiply. Yet, as the figure illustrates, by removing five additional genes we can turn on the biomass flux. Therefore, counterintuitively, we can revive a dead organism through the removal of further genes, a phenomena called the *Lazarus effect* [41].

CASE STUDY: ESTIMATING ROBUSTNESS

The European power grid is an ensemble of more than twenty national power grids consisting of over 3,000 generators and substations (nodes) and 200,000 km of transmission lines (Figure 8.26a-d). The network's degree distribution can be approximated with (Figure 8.26e) [42, 43]

$$p_k = \frac{e^{-k/\langle k \rangle}}{\langle k \rangle} \tag{8.19}$$

indicating that its topology is characterized by a single parameter, $\langle k \rangle$. Such exponential p_k emerges in growing networks that lack preferential attachment (SECTION 5.5).

By knowing $\langle k \rangle$ for each national power grid, we can predict the respective network's critical threshold f_c^{targ} for attacks. As Figure 8.26f shows, for national power grids with $\langle k \rangle > 1.5$ there is a reasonable agreement between the observed and the predicted f_c^{targ} (Group 1). However, for power grids with $\langle k \rangle < 1.5$ (Group 2) the predicted f_c^{targ} underestimates the real f_c^{targ}, indicating that these national networks are more robust to attacks than expected based on their degree distribution. As we show next, this enhanced robustness correlates with the reliability of the respective national networks.

To test the relationship between robustness and reliability, we use several quantities, collected and reported for each power failure: (1) energy not supplied; (2) total loss of power; (3) average interruption time, measured in minutes per year. The measurements indicate that Group 1 networks, for which the real and the theoretical f_c^{targ} agree, represent two thirds of the full network size and carry almost as much power and energy as the Group 2 networks. Yet, Group 1 accumulates more than five times the average interruption time, more than two times the recorded power losses and almost four times the undelivered energy compared to Group 2 [42]. Hence, the national power grids in Group 1 are significantly more fragile than the power grids in Group 2. This result offers direct evidence that networks that are topologically more robust are also more reliable. At the same time this finding is rather counterintuitive: One would expect the denser networks to be more robust. We find, however, that the sparser power grids display enhanced robustness.

In summary, a better understanding of the network topology is essential to improve the robustness of complex systems. We can enhance robustness by either designing network topologies that are simultaneously robust to both random failures and attacks, or by interventions that limit the spread of cascading failures.

These results may suggest that we should redesign the topology of the Internet and the power grid to enhance their robustness [44]. Given the opportunity to do so, this could indeed be achieved. Yet, these infrastructural networks were built incrementally over decades, following the self-organized growth process described in the previous chapters. Given the enormous cost of each node and link, it is unlikely that we would ever be given a chance to rebuild them.

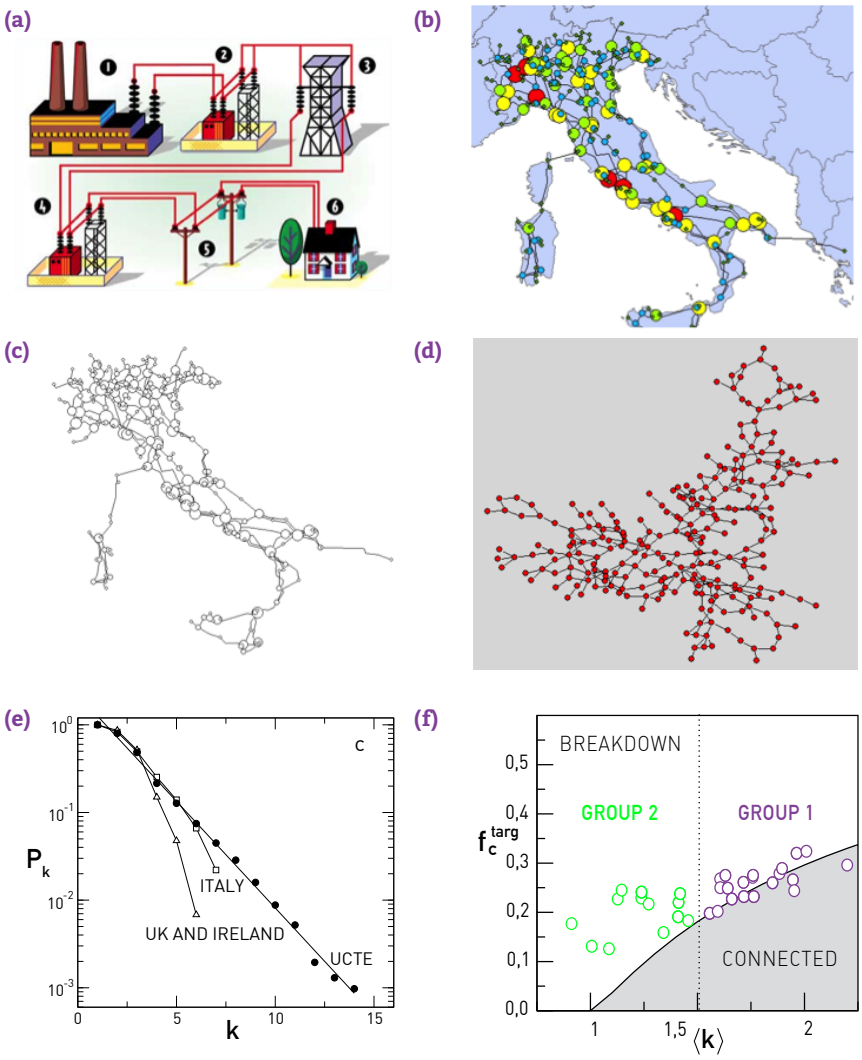


Figure 8.26
The Power Grid

(a) The power grid is a complex infrastructure consisting of (1) power generators, (2) switching units, (3) the high voltage transmission grid, (4) transformers, (5) low voltage lines, (6) consumers, like households or businesses. When we study the network behind the power grid, many of these details are ignored.

(b,c,d) The Italian power grid with the details of production and consumption. Once we strip these details from the network, we obtain the spatial network shown in (c). Once the spatial information is also removed, we arrive to the network (d), which is the typical object of study at the network level.

(e) The complementary cumulative degree distribution P_k of the European power grid. The plot shows the data for the full network (UCTE) and separately for Italy, and the joint network of UK and Ireland, indicating that the national grid's P_k also follows (8.19).

(f) The phase space $(f_c^{\text{targ}}, \langle k \rangle)$ of exponential uncorrelated networks under attack, where f_c^{targ} is the fraction of hubs we must remove to fragment the network. The continuous curve corresponds to the critical boundary for attacks, below which the network retains its giant component. The plot also shows the estimated $f_c^{\text{targ}}(\langle k \rangle)$ for attacks for the thirty-three national power grids within EU, each shown as a separate circle. The plot indicates the presence of two classes of power grids. For countries with $\langle k \rangle > 1.5$ (Group 1), the analytical prediction for f_c^{targ} agrees with the numerically observed values. For countries with $\langle k \rangle < 1.5$ (Group 2) the analytical prediction underestimates the numerically observed values. Therefore, Group 2 national grids show enhanced robustness to attacks, meaning that they are more robust than expected for a random network with the same degree sequence. After [42].

SUMMARY: ACHILLES' HEEL

The masterminds of the September 11, 2001 did not choose their targets at random: the World Trade Center in New York, the Pentagon, and the White House (an intended target) in Washington DC are the hubs of America's economic, military, and political power [45]. Yet, while causing a human tragedy far greater than any other event America has experienced since the Vietnam war, the attacks failed to topple the network. They did offer, however, an excuse to start new wars, like the Iraq and the Afghan wars, triggering a series of cascading events whose impact was far more devastating than the 9/11 terrorist attacks themselves. Yet, all networks, ranging from the economic to the military and the political web, survived. Hence, we can view 9/11 as a tale of robustness and network resilience (BOX 8.5). The roots of this robustness were uncovered in this chapter: Real networks have a whole hierarchy of hubs. Taking out any one of them is not sufficient to topple the underlying network.

The remarkable robustness of real networks represents good news for most complex systems. Indeed, there are uncountable errors in our cells, from misfolding proteins to the late arrival of a transcription factor. Yet, the robustness of the underlying cellular network allows our cells to carry on their normal functions. Network robustness also explains why we rarely notice the effect of router errors on the Internet or why the disappearance of a species does not result in an immediate environmental catastrophe.

This topological robustness has its price, however: fragility against attacks. As we showed in this chapter, the simultaneous removal of several hubs will break any network. This is bad news for the Internet, as it allows crackers to design strategies that can harm this vital communication system. It is bad news for economic systems, as it indicates that hub removal can cripple the whole economy, as vividly illustrated by the 2009 financial meltdown. Yet, it is good news for drug design, as it suggests that an accurate map of cellular networks can help us develop drugs that can kill unwanted bacteria or cancer cells.

The message of this chapter is simple: Network topology, robustness,

BOX 8.5

ROBUSTNESS, RESILIENCE, REDUNDANCY

Redundancy and resilience are concepts deeply linked to robustness. It is useful to clarify the differences between them.

Robustness
A system is robust if it can maintain its basic functions in the presence of internal and external errors. In a network context robustness refers to the system's ability to carry out its basic functions even when some of its nodes and links may be missing.

Resilience
A system is resilient if it can adapt to internal and external errors by changing its mode of operation, without losing its ability to function. Hence resilience is a dynamical property that requires a shift in the system's core activities.

Redundancy
Redundancy implies the presence of parallel components and functions that, if needed, can replace a missing component or funciton. Networks show considerable redundancy in their ability to navigate information between two nodes, thanks to the multiple independent paths between most node pairs.

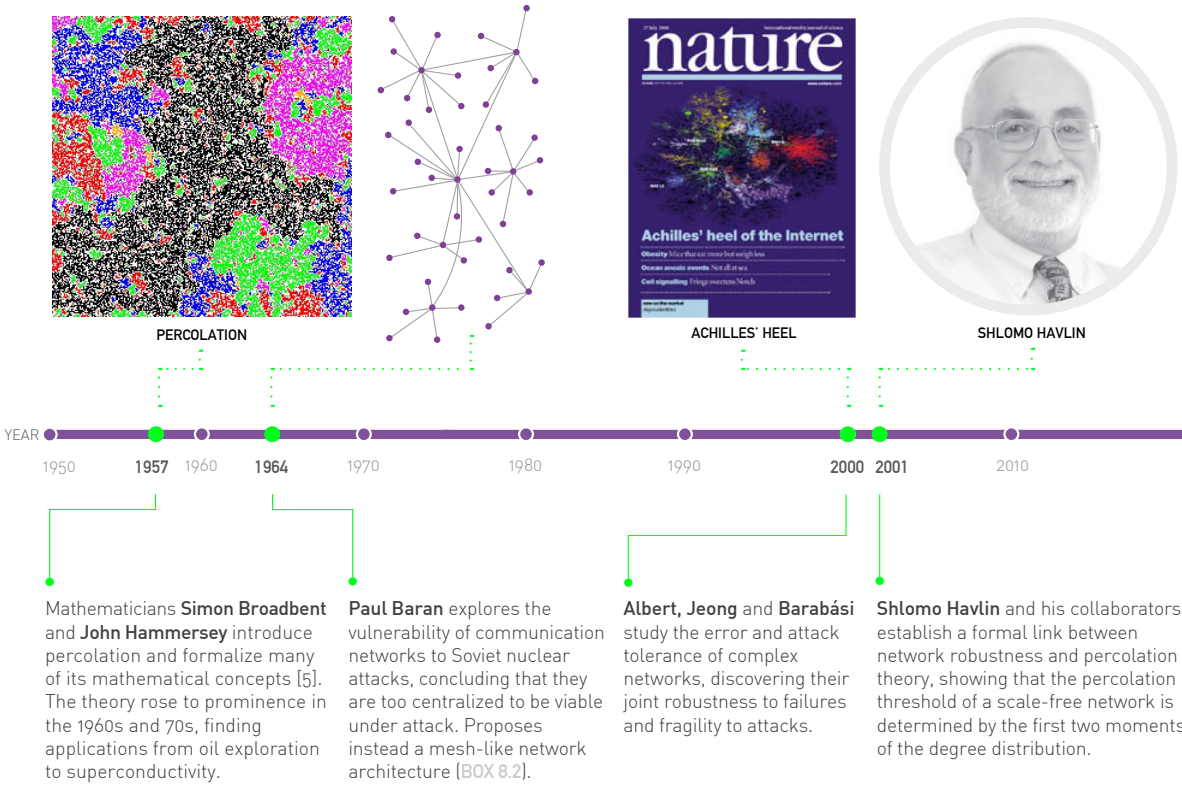


Figure 8.27
From Percolation to Robustness: A Brief History

The systematic study of network robustness started with a paper published in *Nature* (Figure 8.1) by Réka Albert, Hawoong Jeong and Albert-László Barabási [1], reporting the robustness of scale-free networks to random failures and their fragility to attacks. Yet, the analytical understanding of network robustness relies on percolation theory. In this context, particularly important were the contributions of Shlomo Havlin and collaborators, who established the formal link between robustness and percolation theory and showed that the percolation threshold of a scale-free network is determined by the moments of the degree distribution. A statistical physicist from Israel, Havlin had multiple contributions to the study of networks, from discovering the self-similar nature of real networks [46] to exploring the robustness of layered networks [47].

and fragility cannot be separated from one other. Rather, each complex system has its own *Achilles' Heel*: the networks behind them are simultaneously robust to random failures but vulnerable to attacks.

When considering robustness, we cannot ignore the fact that most systems have numerous controls and feedback loops that help them survive in the face of errors and failures. Internet protocols were designed to 'route around the trouble', guiding the traffic away from routers that malfunction; cells have numerous mechanisms to dismantle faulty proteins and to shut down malfunctioning genes. This chapter documented a new contribution to robustness: the structure of the underlying network offers a system an enhanced failure tolerance.

The robustness of scale-free networks prompts us to ask: Could this enhanced robustness be the reason why many real networks are scale-free? Perhaps real systems have developed a scale-free architecture to satisfy their need for robustness. If this hypothesis is correct we should be able to set robustness as an optimization criteria and obtain a scale-free network. Yet, as we showed in SECTION 8.7, a network with maximal robustness has a hub-and-spoke topology. Its degree distribution is bimodal, rather than a power law. This suggests that robustness is not the principle that drives the development of real networks. Rather, networks are scale-free thanks to growth and preferential attachment. It so happens that scale-free networks also have enhanced robustness. Yet, they are not the most robust networks we could design.

BOX 8.6

AT A GLANCE: NETWORK ROBUSTNESS

Malloy-Reed criteria:

A giant component exists if

$$\frac{\langle k^2 \rangle}{\langle k \rangle} > 2$$

Random failures:

$$f_c = 1 - \frac{1}{\frac{\langle k^2 \rangle}{\langle k \rangle} - 1}$$

Random Network: $f_c^{ER} = 1 - \frac{1}{\langle k \rangle}$

Enhanced robustness: $f_c > f_c^{ER}$

Attacks:

$$f_c^{\frac{2-\gamma}{1-\gamma}} = 2 + \frac{2-\gamma}{3-\gamma} k_{min} (f_c^{\frac{3-\gamma}{1-\gamma}} - 1)$$

Cascading failures:

$$p(s) \sim s^{-\alpha}$$

$$\alpha = \begin{cases} 3/2 & \gamma > 3 \\ \frac{\gamma}{\gamma - 1} & 2 < \gamma < 3 \end{cases}$$

HOMEWORK

8.1. Random Failure: Beyond Scale-Free Networks

Calculate the critical threshold f_c for networks with

(a) Power law with exponential cutoff.

(b) Lognormal distribution.

(c) Delta distribution (all nodes have the same degree).

Assume that the networks are uncorrelated and infinite. Refer to Table 4.2 for the functional form of the distribution and the corresponding first and second moments. Discuss the consequences of the obtained results for network robustness.

8.2. Critical Threshold in Correlated Networks

Generate three networks with 10^4 nodes, that are assortative, disassortative and neutral and have a power-law degree distribution with degree exponent $\gamma = 2.2$. Use the Xalvi-Brunet & Sokolov algorithm described in SECTION 7.5 to generate the networks. With the help of a computer, study the robustness of the three networks against random failures, and compare their $P_\infty(f)/P_\infty(0)$ ratio. Which network is the most robust? Can you explain why?

8.3. Failure of Real Networks

Determine the number of nodes that need to fail to break the networks listed in Table 4.1. Assume that each network is uncorrelated.

8.4. Conspiracy in Social Networks

In a Big Brother society, the thought police wants to follow a "divide and conquer" strategy by fragmenting the social network into isolated components. You belong to the resistance and want to foil their plans. There are rumours that the police wants to detain individuals that have many friends and individuals whose friends tend to know each other. The resistance puts you in charge to decide which individuals to protect: those whose friendship circle is highly interconnected or those with many friends. To decide

you simulate two different attacks on your network, by removing (i) the nodes that have the highest clustering coefficient and (ii) the nodes that have the largest degree. Study the size of the giant component in function of the fraction of removed nodes for the two attacks on the following networks:

(a) A network with $N = 10^4$ nodes generated with the configuration model (SECTION 4.8) and power-law degree distribution with $\gamma = 2.5$.

(b) A network with $N = 10^4$ nodes generated with the hierarchical model described in Figure 9.16 and ADVANCED TOPIC 9.B.

Which is the most sensitive topological information, clustering coefficient or degree, which, if protected, limits the damage best? Would it be better if all individuals' information (clustering coefficient, degree, etc.) could be kept secret? Why?

8.5. Avalanches in Networks

Generate a random network with the Erdős-Rényi $G(N,p)$ model and a scale-free network with the configuration model, with $N = 10^3$ nodes and average degree $\langle k \rangle = 2$. Assume that on each node there is a bucket which can hold as many sand grains as the node degree. Simulate then the following process:

(a) At each time step add a grain to a randomly chosen node i.

(b) If the number of grains at node i reaches or exceeds its bucket size, then it becomes unstable and all the grains at the node topple to the buckets of its adjacent nodes.

(c) If this toppling causes any of the adjacent nodes' buckets to be unstable, subsequent topplings follow on those nodes, until there is no unstable bucket left. We call this sequence of toppings an avalanche, its size s being equal to the number of nodes that turned unstable following an initial perturbation (adding one grain).

Repeat (a)-(c) 10^4 times. Assume that at each time step a fraction 10^{-4} of sand grains is lost in the transfer, so that the network buckets do not become saturated with sand. Study the avalanche distribution $P(s)$.

ADVANCED TOPICS 8.A PERCOLATION IN SCALE-FREE NETWORKS

To understand how a scale-free network breaks apart as we approach the threshold (8.7), we need to determine the corresponding critical exponents γ_p, β_p and ν. The calculations indicate that the scale-free property alters the value of these exponents, leading to systematic deviations from the exponents that characterize random networks (SECTION 8.2).

Let us start with the probability P_∞ that a randomly selected node belongs to the giant component. According to (8.2) this follows a power law near p_c (or f_c in the case of node removal). The calculations predict that for a scale-free network the exponent β_p depends on the degree exponent γ as [7, 48, 49, 50, 51]

$$\beta_p = \begin{cases} \dfrac{1}{3-\gamma} & 2 < \gamma < 3, \\ \dfrac{1}{\gamma-3} & 3 < \gamma < 4, \\ 1 & \gamma > 4. \end{cases} \tag{8.20}$$

Hence, while for a random network (corresponding to $\gamma > 4$) we have $\beta_p = 1$, for most scale-free networks of practical interest $\beta_p > 1$. Therefore, the giant component collapses faster in the vicinity of the critical point in a scale-free network than in a random network.

The exponent characterizing the average component size near p_c follows [48]

$$\gamma_p = \begin{cases} 1 & \gamma > 3 \\ -1 & 2 < \gamma < 3. \end{cases} \tag{8.21}$$

The negative γ_p for $\gamma < 3$ may appear surprising. Note, however, that for $\gamma < 3$ we always have a giant component. Hence, the divergence (8.1) cannot be observed in this regime.

For a randomly connected network with arbitrary degree distribution the size distribution of the finite clusters follows [48, 50, 51]

$$n_s \sim s^{-\tau} e^{-s/s^*}. \tag{8.22}$$

Here, n_s is the number of clusters of size s and s^* is the crossover cluster size. At criticality

$$s^* \sim \left| p - p_c \right|^{-\sigma} \tag{8.23}$$

The critical exponents are

$$\tau = \begin{cases} \dfrac{5}{2} & \gamma > 4 \\ \dfrac{2\gamma - 3}{\gamma - 2} & 2 < \gamma < 4, \end{cases} \tag{8.24}$$

$$\sigma = \begin{cases} \dfrac{3-\gamma}{\gamma-2} & 2 < \gamma < 3 \\ \dfrac{\gamma-3}{\gamma-2} & 3 < \gamma < 4 \\ \dfrac{1}{2} & \gamma > 4. \end{cases} \tag{8.25}$$

Once again, the random network values $\tau = 5/2$ and $\sigma = 1/2$ are recovered for $\gamma > 4$.

In summary, the exponents describing the breakdown of a scale-free network depend on the degree exponent γ. This is true even in the range $3 < \gamma < 4$, where the percolation transition occurs at a finite threshold f_c. The mean-field behavior predicted for percolation in infinite dimensions, capturing the response of a random network to random failures, is recovered only for $\gamma > 4$.

ADVANCED TOPICS 8.B MOLLOY-REED CRITERION

The purpose of this section is to derive the Molloy-Reed criterion, which allows us to calculate the percolation threshold of an arbitrary network [6]. For a giant component to exist each node that belongs to it must be connected to at least two other nodes on average (Figure 8.8). Therefore, the average degree k_i of a randomly chosen node i that is part of the giant component should be at least 2. Denote with $P(k_i \mid i \leftrightarrow j)$ the conditional probability that a node in a network with degree k_i is connected to a node j that is part of the giant component. This conditional probability allows us to determine the expected degree of node i as [51]

$$\langle k_i \mid i \leftrightarrow j \rangle = \sum_{k_i} k_i P(k_i \mid i \leftrightarrow j) = 2 \,. \tag{8.26}$$

In other words, $\langle k_i \mid i \leftrightarrow j \rangle$ should be equal or exceed two, the condition for node i to be part of the giant component. We can write the probability appearing in the sum (8.26) as

$$P(k_i \mid i \leftrightarrow j) = \frac{P(k_i, i \leftrightarrow j)}{P(i \leftrightarrow j)} = \frac{P(i \leftrightarrow j \mid k_i) p(k_i)}{P(i \leftrightarrow j)} \,, \tag{8.27}$$

where we used Bayes' theorem in the last term. For a network with degree distribution p_k, in the absence of degree correlations, we can write

$$P(i \leftrightarrow j) = \frac{2L}{N(N-1)} = \frac{\langle k \rangle}{N-1} \,, \qquad P(i \leftrightarrow j \mid k_i) = \frac{k_i}{N-1} \,, \tag{8.28}$$

which express the fact that we can choose between $N-1$ nodes to link to, each with probability $1/(N-1)$ and that we can try this k_i times. We can now return to (8.26), obtaining

$$\sum_{k_i} k_i P(k_i \mid i \leftrightarrow j) = \sum_{k_i} k_i \frac{P(i \leftrightarrow j \mid k_i) p(k_i)}{P(i \leftrightarrow j)} = \sum_{k_i} k_i \frac{k_i p(k_i)}{\langle k \rangle} = \frac{\sum_{k_i} k_i^2 p(k_i)}{\langle k \rangle} \tag{8.29}$$

With that we arrive at the Molloy-Reed criterion (8.4), providing the condition to have a giant component as

$$\kappa = \frac{\langle k^2 \rangle}{\langle k \rangle} > 2 \,. \tag{8.30}$$

ADVANCED TOPICS 8.C CRITICAL THRESHOLD UNDER RANDOM FAILURES

The purpose of this section is to derive (8.7), that provides the critical threshold for random node removal [7, 51]. The random removal of an f fraction of nodes has two consequences:

- It alters the degree of some nodes, as nodes that were previously connected to the removed nodes will lose some links [$k \to k' \le k$].
- Consequently, it changes the degree distribution, as the neighbors of the missing nodes will have an altered degree [$p_k \to p'_{k'}$].

To be specific, after we randomly remove an f fraction of nodes, a node with degree k becomes a node with degree k' with probability

$$\binom{k}{k'} f^{k-k'}(1-f)^{k'} \qquad k' \le k \,. \tag{8.31}$$

The first f-dependent term in (8.31) accounts for the fact that the selected node lost $(k - k')$ links, each with probability f; the next term accounts for the fact that node removal leaves k' links untouched, each with probability $(1 - f)$.

The probability that we have a degree-k node in the original network is p_k; the probability that we have a new node with degree k' in the new network is

$$p'_{k'} = \sum_{k=k'}^{\infty} p_k \binom{k}{k'} f^{k-k'}(1-f)^{k'} . \tag{8.32}$$

Let us assume that we know $\langle k \rangle$ and $\langle k^2 \rangle$ for the original degree distribution p_k. Our goal is to calculate $\langle k' \rangle$, $\langle k'^2 \rangle$ for the new degree distribution $p'_{k'}$, obtained after we randomly removed an f fraction of the nodes. For this we write

$$\begin{aligned}\langle k'\rangle_f &= \sum_{k'=0}^{\infty} k' p_{k'} \\ &= \sum_{k'=0}^{\infty} k' \sum_{k=k'}^{\infty} p_k \left(\frac{k!}{k'!(k-k')!}\right) f^{k-k'}(1-f)^{k'} \\ &= \sum_{k'=0}^{\infty} \sum_{k=k'}^{\infty} p_k \frac{k(k-1)!}{(k'-1)!(k-k')!} f^{k-k'}(1-f)^{k'-1}(1-f).\end{aligned} \tag{8.33}$$

The sum above is performed over the triangle shown in Figure 8.28. We can check that we are performing the same sum if we change the order of summation together with the limits of the sums as

$$\sum_{k'=0}^{\infty} \sum_{k=k'}^{\infty} = \sum_{k=0}^{\infty} \sum_{k'=0}^{k}. \tag{8.34}$$

Hence we obtain

$$\begin{aligned}\langle k'\rangle_f &= \sum_{k=0}^{\infty} k' \sum_{k'=0}^{k} p_k \frac{k(k-1)!}{(k'-1)!(k-k')!} f^{k-k'}(1-f)^{k'-1}(1-f) \\ &= \sum_{k=0}^{\infty}(1-f)kp_k \sum_{k'=0}^{k} \frac{(k-1)!}{(k'-1)!(k-k')!} f^{k-k'}(1-f)^{k'-1} \\ &= \sum_{k=0}^{\infty}(1-f)kp_k \sum_{k'=0}^{k} \binom{k-1}{k'-1} f^{k-k'}(1-f)^{k'-1} \\ &= \sum_{k=0}^{\infty}(1-f)kp_k \\ &= (1-f)\langle k\rangle.\end{aligned} \tag{8.35}$$

This connects $\langle k' \rangle$ to the original $\langle k \rangle$ after the random removal of an f fraction of nodes.

We perform a similar calculation for $\langle k'^2 \rangle$:

$$\begin{aligned}\langle k'^2\rangle_f &= \langle k'(k'-1)+k'\rangle_f \\ &= \langle k'(k'-1)\rangle_f + \langle k'\rangle_f \\ &= \sum_{k'=0}^{\infty} k'(k'-1)p_{k'} + \langle k'\rangle_f.\end{aligned} \tag{8.36}$$

Again, we change the order of the sums (Figure 8.28), obtaining

$$\begin{aligned}\langle k'(k'-1)\rangle_f &= \sum_{k'=0}^{\infty} k'(k'-1)p_{k'} \\ &= \sum_{k'=0}^{\infty} k'(k'-1) \sum_{k=k'}^{\infty} p_k \binom{k}{k'} f^{k-k'}(1-f)^{k'} \\ &= \sum_{k=0}^{\infty} k'(k'-1) \sum_{k'=0}^{k} p_k \frac{k'(k'-1)}{k'!(k-k')!} f^{k-k'}(1-f)^{k'} \\ &= \sum_{k=0}^{\infty} \sum_{k'=0}^{k} p_k \frac{k!}{(k'-2)!(k-k')!} f^{k-k'}(1-f)^{k'-2}(1-f)^2 \\ &= \sum_{k=0}^{\infty}(1-f)^2 k(k-1)p_k \sum_{k'=0}^{k} \frac{(k-2)!}{(k'-2)!(k-k')!} f^{k-k'}(1-f)^{k'-2} \\ &= \sum_{k=0}^{\infty}(1-f)^2 k(k-1)p_k \sum_{k'=0}^{k} \binom{k-2}{k'-2} f^{k-k'}(1-f)^{k'-2} \\ &= \sum_{k=0}^{\infty}(1-f)^2 k(k-1)p_k\end{aligned} \tag{8.37}$$

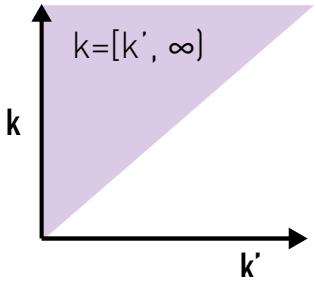


Figure 8.28
The Integration Domain

In (8.34) we change the integration order, *i.e.* the order of the two sums. We can do so because both sums are defined over the triangle shown in purple in the figure.

$$= (1-f)^2 \langle k(k-1) \rangle .$$

Hence we obtain

$$\begin{aligned}
\langle k'^2 \rangle_f &= \langle k'(k'-1) + k' \rangle_f \\
&= \langle k'(k'-1) \rangle_f + \langle k' \rangle_f \\
&= (1-f)^2 \langle k(k-1) \rangle + (1-f)\langle k \rangle \\
&= (1-f)^2 \left(\langle k^2 \rangle - \langle k \rangle \right) + (1-f)\langle k \rangle \\
&= (1-f)^2 \langle k^2 \rangle - (1-f)^2 \langle k \rangle + (1-f)\langle k \rangle \\
&= (1-f)^2 \langle k^2 \rangle - \left(-f^2 + 2f - 1 + 1 - f \right) \langle k \rangle \\
&= (1-f)^2 \langle k^2 \rangle + f(1-f)\langle k \rangle .
\end{aligned} \tag{8.38}$$

which connects $\langle k'^2 \rangle$ to the original $\langle k^2 \rangle$ after the random removal of an f fraction of nodes. Let us put the results (8.35) and (8.38) together:

$$\langle k' \rangle_f = (1-f)\langle k \rangle , \tag{8.39}$$

$$\langle k' \rangle_f = (1-f)^2 \langle k^2 \rangle + f(1-f)\langle k \rangle . \tag{8.40}$$

According to the Molloy-Reed criterion (8.4) the breakdown threshold is given by

$$\kappa = \frac{\langle k'^2 \rangle_f}{\langle k' \rangle_f} = 2 . \tag{8.41}$$

Inserting (8.38) and (8.40) into (8.41) we obtain our final result (8.7),

$$f_c = 1 - \frac{1}{\frac{\langle k^2 \rangle}{\langle k \rangle} - 1} \tag{8.42}$$

providing the breakdown threshold of networks with arbitrary p_k under random node removal.

ADVANCED TOPICS 8.D BREAKDOWN OF A FINITE SCALE-FREE NETWORK

In this section we derive the dependence (8.10) of the breakdown threshold of a scale-free network on the network size N. We start by calculating the m^{th} moment of a power-law distribution

$$\langle k^m \rangle = (\gamma-1)k_{\min}^{\gamma-1}\int_{k_{min}}^{k_{\max}} k^{m-\gamma}dk = \frac{(\gamma-1)}{(m-\gamma+1)}k_{\min}^{\gamma-1}[k^{m-\gamma+1}]_{k_{\min}}^{k_{\max}}. \tag{8.43}$$

Using (4. 18)

$$k_{\max} = k_{\min}N^{\frac{1}{\gamma-1}} \tag{8.44}$$

we obtain

$$\langle k^m \rangle = \frac{(\gamma-1)}{(m-\gamma+1)}k_{\min}^{\gamma-1}[k_{\max}^{m-\gamma+1} - k_{\min}^{m-\gamma+1}]\cdot \tag{8.45}$$

To calculate f_c we need to determine the ratio

$$\kappa = \frac{\langle k^2 \rangle}{\langle k \rangle} = \frac{(2-\gamma)}{(3-\gamma)}\frac{k_{\max}^{3-\gamma} - k_{\min}^{3-\gamma}}{k_{\max}^{2-\gamma} - k_{\min}^{2-\gamma}}, \tag{8.46}$$

which for large N (and hence for large k_{max}) depends on γ as

$$\kappa = \frac{\langle k^2 \rangle}{\langle k \rangle} = \left|\frac{2-\gamma}{3-\gamma}\right| \begin{cases} k_{\min} & \gamma > 3 \\ k_{\max}^{3-\gamma}k_{\min}^{\gamma-2} & 3 > \gamma > 2 \\ k_{\max} & 2 > \gamma > 1 \end{cases} \tag{8.47}$$

The breakdown threshold is given by (8.7)

$$f_c = 1 - \frac{1}{\kappa - 1}, \tag{8.48}$$

where κ is given by (8.46). Inserting (8.43) into (8.42) and (8.47), we obtain

$$f_c \approx 1 - \frac{C}{N^{\frac{3-\gamma}{\gamma-1}}}, \tag{8.49}$$

which is (8.10).

ADVANCED TOPICS 8.E ATTACK AND ERROR TOLERANCE OF REAL NETWORKS

In this section we explore the attack and error curves for the ten reference networks discussed in Tables 4.1 and (8.2). The corresponding curves are shown in Figure 8.29. Their inspection reveals several patterns, confirming the results discussed in this chapter:

- For all networks the error and attack curves separate, confirming the Achilles' Heel property (SECTION 8.8): Real networks are robust to random failures but are fragile to attacks.

- The separation between the error and attack curves depends on the average degree and the degree heterogeneity of each network. For example, for the citation and the actor networks f_c for the attacks is in the vicinity of 0.5 and 0.75, respectively, rather large values. This is because these networks are rather dense, with $\langle k \rangle = 20.8$ for citation network and $\langle k \rangle = 83.7$ for the actor network. Hence these networks can survive the removal of a very high fraction of their hubs.

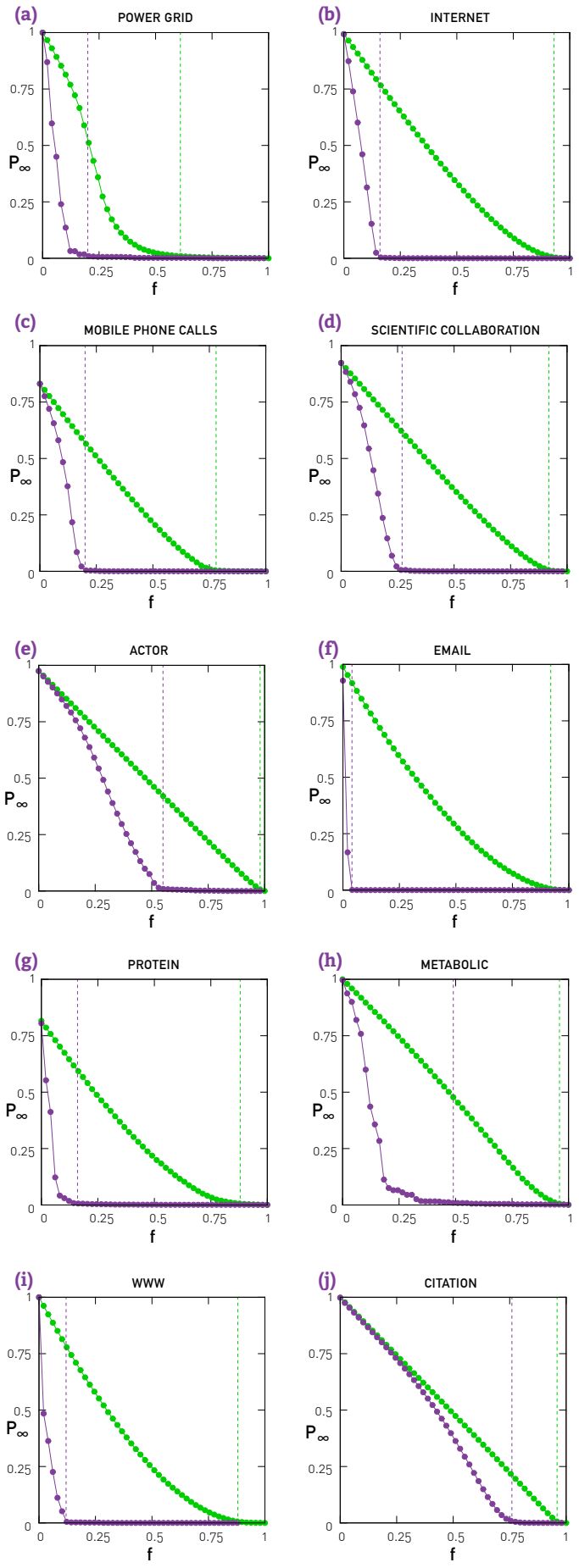


Figure 8.29

Error and Attack Curves

The error (green) and attack (purple) curves for the ten reference networks listed in Table 4.1. The green vertical line corresponds to the estimated f_c^{rand} for errors, while the purple vertical line corresponds to f_c^{targ} for attacks. The estimated f_c corresponds to the point where the giant component first drops below 1% of its original size. In most systems this procedure offers a good approximation for f_c. The only exception is the metabolic network, for which $f_c^{targ} < 0.25$, but a small cluster persists, pushing the reported f_c^{targ} to $f_c^{targ} \simeq 0.5$.

ADVANCED TOPICS 8.F ATTACK THRESHOLD

The goal of this section is to derive (8.12), providing the attack threshold of a scale-free network. We aim to calculate f_c for an uncorrelated scale-free network, generated by the configuration model with $p_k = c \cdot k^{-\gamma}$ where $k = k_{\min}, \ldots, k_{\max}$ and $c \approx (\gamma - 1)/(k_{\min}^{-\gamma+1} - k_{\max}^{-\gamma+1})$.

The removal of an f fraction of nodes in a decreasing order of their degree (hub removal) has two effects [9, 51]:

(i) The maximum degree of the network changes from $k_{\max}$ to $k'_{\max}$.

(ii) The links connected to the removed hubs are also removed, changing the degree distribution of the remaining network.

The resulting network is still uncorrelated, therefore we can use the Molloy-Reed criteria to determine the existence of a giant component.

We start by considering the impact of (i). The new upper cutoff, $k'_{\max}$, is given by

$$f = \int_{k'_{\max}}^{k_{\max}} p_k dk = \frac{\gamma - 1}{\gamma - 1} \frac{k'^{-\gamma+1}_{\max} - k^{-\gamma+1}_{\max}}{k^{-\gamma+1}_{\min} - k^{-\gamma+1}_{\max}}. \tag{8.50}$$

If we assume that $k_{\max} \gg k'_{\max}$ and $k_{\max} \gg k_{\min}$ (true for large scale-free networks with natural cutoff), we can ignore the $k_{\max}$ terms, obtaining

$$f = \left(\frac{k'_{\max}}{k_{\min}} \right)^{-\gamma+1}, \tag{8.51}$$

which leads to

$$k'_{\max} = k_{\min} f^{\frac{1}{1-\gamma}}. \tag{8.52}$$

Equation (8.52) provides the new maximum degree of the network after we remove an f fraction of the hubs.

Next we turn to (ii), accounting for the fact that hub removal changes the degree distribution $p_k \rightarrow p'_k$. In the absence of degree correlations we assume that the links of the removed hubs connect to randomly selected stubs. Consequently, we calculate the fraction of links removed 'randomly', $\tilde{f}$, as a consequence of removing an f fraction of the hubs:

$$\tilde{f} = \frac{\int_{k'_{\max}}^{k_{\max}} kp_k dk}{\langle k \rangle} = \frac{1}{\langle k \rangle} c \int_{k'_{\max}}^{k_{\max}} k^{-\gamma+1} dk$$
$$= \frac{1}{\langle k \rangle} \frac{1-\gamma}{2-\gamma} \frac{k'^{-\gamma+2}_{\max} - k^{-\gamma+2}_{\max}}{k^{-\gamma+1}_{\min} - k^{-\gamma+2}_{\max}} . \quad (8.53)$$

Ignoring the $k_{\max}$ term again and using $\langle k \rangle \approx \frac{\gamma-1}{\gamma-2} k_{\min}$ we obtain

$$\tilde{f} = \left(\frac{k'_{\max}}{k_{\min}} \right)^{-\gamma+2} . \quad (8.54)$$

Using (8.51) we obtain

$$\tilde{f} = f^{\frac{2-\gamma}{1-\gamma}} . \quad (8.55)$$

For $\gamma \rightarrow 2$ we have $\tilde{f} \rightarrow 1$, which means that the removal of a tiny fraction of the hubs removes all links, potentially destroying the network. This is consistent with the finding of CHAPTER 4 that for $\gamma = 2$ the hubs dominate the network.

In general the degree distribution of the remaining network is

$$p'_{k'} = \sum_{k=k_{\min}}^{k'_{\max}} \binom{k}{k'} \tilde{f}^{k-k'} (1-\tilde{f})^{k'} p_k . \quad (8.56)$$

Note that we obtained the degree distribution (8.32) in ADVANCED TOPICS 8.C. This means that now we can proceed with the calculation method developed there for random node removal. To be specific, we calculate κ for a scale-free network with $k_{\min}$ and $k'_{\max}$ using (8.45):

$$\kappa = \frac{2-\gamma}{3-\gamma} \frac{k'^{3-\gamma}_{\max} - k^{3-\gamma}_{\min}}{k'^{2-\gamma}_{\max} - k^{2-\gamma}_{\min}} . \quad (8.57)$$

Substituting into this (8.52) we have

$$\kappa = \frac{2-\gamma}{3-\gamma} \frac{k^{3-\gamma}_{\min} f^{(3-\gamma)/(1-\gamma)} - k^{3-\gamma}_{\min}}{k^{2-\gamma}_{\min} f^{(2-\gamma)/(1-\gamma)} - k^{2-\gamma}_{\min}} = \frac{2-\gamma}{3-\gamma} k_{\min} \frac{f^{(3-\gamma)/(1-\gamma)} - 1}{f^{(2-\gamma)/(1-\gamma)} - 1} . \quad (8.58)$$

After simple transformations we obtain

$$f_c^{\frac{2-\gamma}{1-\gamma}} = 2 + \frac{2-\gamma}{3-\gamma} k_{\min} \left(f_c^{\frac{3-\gamma}{1-\gamma}} - 1 \right) \quad (8.59)$$

ADVANCED TOPICS 8.G THE OPTIMAL DEGREE DISTRIBUTION

In this section we derive the bimodal degree distribution that simultaneously optimizes a network's topology against attacks and failures, as discussed in SECTION 8.7 [37]. Let us assume, as we did in (8.17), that the degree distribution is bimodal, consisting of two delta functions:

$$p_k = (1-r)\delta(k-k_{\min}) + r\delta(k-k_{\max}). \tag{8.62}$$

We start by calculating the total threshold, f^{tot}, as a function of r and $k_{\max}$ for a fixed $\langle k\rangle$. To obtain analytical expressions for f_c^{rand} and f_c^{targ} we calculate the moments of the bimodal distribution (8.62),

$$\begin{aligned} \langle k\rangle &= (1-r)k_{\min} + rk_{\max}, \\ \langle k^2\rangle &= (1-r)k_{\min}^2 + rk_{\max}^2 = \frac{(\langle k\rangle - rk_{\max})^2}{1-r} + rk_{\max}^2. \end{aligned} \tag{8.63}$$

Inserting these into (8.7) we obtain

$$f_c^{\text{rand}} = \frac{\langle k\rangle^2 - 2r\langle k\rangle k_{\max} - 2(1-r)\langle k\rangle + rk_{\max}^2}{\langle k\rangle^2 - 2r\langle k\rangle k_{\max} - (1-r)\langle k\rangle + rk_{\max}^2}. \tag{8.64}$$

To determine the threshold for targeted attack, we must consider the fact that we have only two types of nodes, i.e. an r fraction of nodes have degree $k_{\max}$ and the remaining $(1-r)$ fraction have degree $k_{\min}$. Hence hub removal can either remove all hubs (case (i)), or only some fraction of them (case (ii)):

(i) $f_c^{\text{targ}} > r$. In this case all hubs have been removed, hence the nodes left after the targeted attack have degree $k_{\min}$. We therefore obtain

$$f_c^{\text{targ}} = r + \frac{1-r}{\langle k\rangle - rk_{\max}}\left\{\langle k\rangle \frac{\langle k\rangle - rk_{\max} - 2(1-r)}{\langle k\rangle - rk_{\max} - (1-r)} - rk_{\max}\right\}. \tag{8.65}$$

(ii) $f_c^{\text{targ}} < r$. In this case the removed nodes are all from the high-degree group, leaving behind some $k_{\max}$ nodes. Hence we obtain

$$f_c^{\text{targ}} = \frac{\langle k\rangle^2 - 2r\langle k\rangle k_{\max} + rk_{\max}^2 - 2(1-r)\langle k\rangle}{k_{\max}(k_{\max}-1)(1-r)}. \tag{8.66}$$

With the thresholds (8.64) - (8.66) we can now evaluate the total threshold f_c^{tot} (8.16). To obtain an expression for the optimal value of $k_{\max}$ as a function of r we determine the value of k for which f_c^{tot} is maximal. Using (8.64) and (8.66), we find that for small r the optimal value of $k_{\max}$ can be approximated by

$$k_{\max} \sim \left\{\frac{2\langle k\rangle^2(\langle k\rangle - 1)^2}{2\langle k\rangle - 1}\right\}^{1/3} r^{-2/3} = Ar^{-2/3}. \tag{8.67}$$

Using this result and (8.16), for small r we have

$$f_c^{\text{tot}} = 2 - \frac{1}{\langle k\rangle - 1} - \frac{3\langle k\rangle}{A^2} r^{1/3} + O(r^{2/3}). \tag{8.68}$$

Thus f_c^{tot} approaches the theoretical maximum when r approaches zero. For a network of N nodes the maximum value of f_c^{tot} is obtained when $r = 1/N$, being the smallest value consistent with having at least one node of degree $k_{\max}$. Given this r the equation determining the optimal $k_{\max}$, representing the size of the central hubs, is [37]

$$k_{\max} = AN^{2/3}, \tag{8.69}$$

where A is defined in (8.67).

BIBLIOGRAPHY

[1] R. Albert, H. Jeong, and A.-L. Barabási. Attack and error tolerance of complex networks. Nature, 406: 378, 2000.

[2] D. Stauffer and A. Aharony. *Introduction to Percolation Theory*. Taylor and Francis. London, 1994.

[3] A. Bunde and S. Havlin. *Fractals and Disordered Systems*. Springer, 1996.

[4] B. Bollobás and O. Riordan. *Percolation*. Cambridge University Press. Cambridge, 2006.

[5] S. Broadbent and J. Hammersley. Percolation processes I. Crystals and mazes. Proceedings of the Cambridge Philosophical Society, 53: 629, 1957.

[6] M. Molloy and B. Reed. A criticial point for random graphs with a given degree sequence. Random Structures and Algorithms, 6: 161, 1995.

[7] R. Cohen, K. Erez, D. ben-Avraham and S. Havlin. Resilience of the Internet to random breakdowns. Phys. Rev. Lett., 85: 4626, 2000.

[8] D. S. Callaway, M. E. J. Newman, S. H. Strogatz. and D. J. Watts. Network robustness and fragility: Percolation on random graphs. Phys. Rev. Lett., 85: 5468–5471, 2000.

[9] R. Cohen, K. Erez, D. ben-Avraham and S. Havlin. Breakdown of the Internet under intentional attack. Phys. Rev. Lett., 86: 3682, 2001.

[10] B. Bollobás and O. Riordan. Robustness and Vulnerability of Scale-Free Random Graphs. Internet Mathematics, 1: 1-35, 2003.

[11] P. Baran. Introduction to Distributed Communications Networks. Rand Corporation Memorandum, RM-3420-PR, 1964.

[12] D.N. Kosterev, C.W. Taylor and W.A. Mittlestadt. Model Validation of the August 10, 1996 WSCC System Outage. IEEE Transactions on Power Systems 14: 967-979, 1999.

[13] C. Labovitz, A. Ahuja and F. Jahasian. Experimental Study of Internet Stability and Wide-Area Backbone Failures. Proceedings of IEEE FTCS, Madison, WI, 1999.

[14] A. G. Haldane and R. M. May. Systemic risk in banking ecosystems. Nature, 469: 351-355, 2011.

[15] T. Roukny, H. Bersini, H. Pirotte, G. Caldarelli and S. Battiston. Default Cascades in Complex Networks: Topology and Systemic Risk. Scientific Reports, 3: 2759, 2013.

[16] G. Tedeschi, A. Mazloumian, M. Gallegati, and D. Helbing. Bankruptcy cascades in interbank markets. PLoS One, 7: e52749, 2012.

[17] D. Helbing. Globally networked risks and how to respond. Nature, 497: 51-59, 2013.

[18] I. Dobson, B. A. Carreras, V. E. Lynch and D. E. Newman. Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization. CHAOS, 17: 026103, 2007.

[19] E. Bakshy, J. M. Hofman, W. A. Mason, and D. J. Watts. Everyone's an influencer: quantifying influence on twitter. Proceedings of the fourth ACM international conference on Web search and data mining (WSDM '11). ACM, New York, NY, USA, 65-74, 2011.

[20] Y. Y. Kagan. Accuracy of modern global earthquake catalogs. Phys. Earth Planet. Inter., 135: 173, 2003.

[21] M. Nagarajan, H. Purohit, and A. P. Sheth. A Qualitative Examination of Topical Tweet and Retweet Practices. ICWSM, 295-298, 2010.

[22] P. Fleurquin, J.J. Ramasco and V.M. Eguiluz. Systemic delay propagation in the US airport network. Scientific Reports, 3: 1159, 2013.

[23] B. K. Ellis, J. A. Stanford, D. Goodman, C. P. Stafford, D.L. Gustafson, D. A. Beauchamp, D. W. Chess, J. A. Craft, M. A. Deleray, and B. S. Hansen. Long-term effects of a trophic cascade in a large lake ecosystem. PNAS, 108: 1070, 2011.

[24] V. R. Sole, M. M. Jose. Complexity and fragility in ecological networks. Proc. R. Soc. Lond. B, 268: 2039, 2001.

[25] F. Jordán, I. Scheuring and G. Vida. Species Positions and Extinction Dynamics in Simple Food Webs. Journal of Theoretical Biology, 215: 441-

448, 2002.

[26] S.L. Pimm and P. Raven. Biodiversity: Extinction by numbers. Nature, 403: 843, 2000.

[27] World Economic Forum, *Building Resilience in Supply Chains*. World Economic Forum, 2013.

[28] Joint Economic Committee of US Congress. Your flight has been delayed again: Flight delays cost passengers, airlines and the U.S. economy billions. Available at http://www.jec.senate.gov, May 22. 2008.

[29] I. Dobson, A. Carreras, and D.E. Newman. A loading dependent model of probabilistic cascading failure. Probability in the Engineering and Informational Sciences, 19: 15, 2005.

[30] D.J. Watts. A simple model of global cascades on random networks. PNAS, 99: 5766, 2002.

[31] K.-I. Goh, D.-S. Lee, B. Kahng, and D. Kim. Sandpile on scale-free networks. Phys. Rev. Lett., 91: 148701, 2003.

[32] D.-S. Lee, K.-I. Goh, B. Kahng, and D. Kim. Sandpile avalanche dynamics on scale-free networks. Physica A, 338: 84, 2004.

[33] M. Ding and W. Yang. Distribution of the first return time in fractional Brownian motion and its application to the study of onoff intermittency. Phys. Rev. E., 52: 207-213, 1995.

[34] A. E. Motter and Y.-C. Lai. Cascade-based attacks on complex networks. Physical Review E, 66: 065102, 2002.

[35] Z. Kong and E. M. Yeh. Resilience to Degree-Dependent and Cascading Node Failures in Random Geometric Networks. IEEE Transactions on Information Theory, 56: 5533, 2010.

[36] G. Paul, S. Sreenivas, and H. E. Stanley. Resilience of complex networks to random breakdown. Phys. Rev. E, 72: 056130, 2005.

[37] G. Paul, T. Tanizawa, S. Havlin, and H. E. Stanley. Optimization of robustness of complex networks. European Physical Journal B, 38: 187–191, 2004.

[38] A.X.C.N. Valente, A. Sarkar, and H. A. Stone. Two-peak and three-peak optimal complex networks. Phys. Rev. Lett., 92: 118702, 2004.

[39] T. Tanizawa, G. Paul, R. Cohen, S. Havlin, and H. E. Stanley. Optimization of network robustness to waves of targeted and random attacks. Phys. Rev. E, 71: 047101, 2005.

[40] A.E. Motter. Cascade control and defense in complex networks. Phys. Rev. Lett., 93: 098701, 2004.

[41] A. Motter, N. Gulbahce, E. Almaas, and A.-L. Barabási. Predicting synthetic rescues in metabolic networks. Molecular Systems Biology, 4: 1-10, 2008.

[42] R.V. Sole, M. Rosas-Casals, B. Corominas-Murtra, and S. Valverde. Robustness of the European power grids under intentional attack. Phys. Rev. E, 77: 026102, 2008.

[43] R. Albert, I. Albert, and G.L. Nakarado. Structural Vulnerability of the North American Power Grid. Phys. Rev. E, 69: 025103 R, 2004.

[44] C.M. Schneider, N. Yazdani, N.A.M. Araújo, S. Havlin and H.J. Herrmann. Towards designing robust coupled networks. Scientific Reports, 3: 1969, 2013.

[45] A.-L. Barabási. *Linked: The New Science of Networks*. Plume, New York, 2002.

[46] C.M. Song, S. Havlin, and H.A Makse. Self-similarity of complex networks. Nature, 433: 392, 2005.

[47] S.V. Buldyrev, R. Parshani, G. Paul, H.E. Stanley and S. Havlin. Catastrophic cascade of failures in interdependent networks. Nature, 464: 08932, 2010.

[48] R. Cohen, D. ben-Avraham and S. Havlin. Percolation critical exponents in scale-free networks. Phys. Rev. E, 66: 036113, 2002.

[49] S. N. Dorogovtsev, J. F. F. Mendes, and A. N. Samukhin. Anomalous percolation properties of growing networks. Phys. Rev. E, 64: 066110, 2001.

[50] M. E. J. Newman, S. H. Strogatz, and D. J. Watts. Random graphs with arbitrary degree distributions and their applications. Phys. Rev. E, 64: 026118, 2001.

[51] R. Cohen and S. Havlin. *Complex Networks: Structure, Robustness and Function*. Cambridge University Press. Cambridge, UK, 2010.