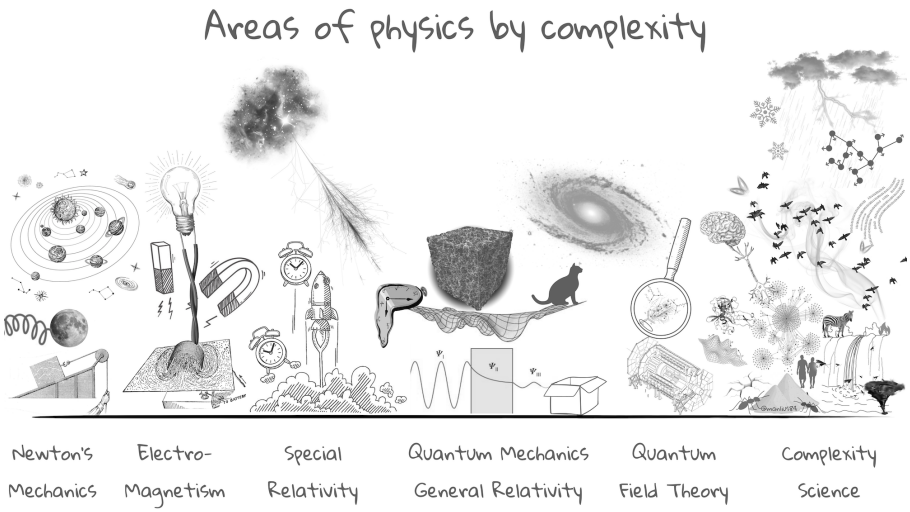
Final Report

Physics of Complex Networks: Structure and Dynamics

Università degli Studi di Padova



Project #5: Cascade Failures

Davide Bacilieri, Tommaso Bertola, Guglielmo Bordin, Maximilian Matzler, Alessio Pitteri, Marco Zenari

Erdőstroyers

Last update: July 23, 2023

Contents

1 | Motter-Lai model

Task leader(s): *Tommaso Bertola*

1.1 | Introduction to cascade-based attacks

Nowadays complex networks are ubiquitous in both the real world and scientific literature, as they share surprising characteristics related to their structure. Some relevant properties are the organized structures emerging from the connections, the typical scale-free degree distributions and the small average distances between nodes even when the network is far from being fully connected, the so-called *small-worldness*.

However, when the network is perturbed by the removal of some targeted nodes, fragile behaviors emerge when the dynamics of the network is taken into account. This phenomenon is referred to by the *robust-yet-fragile* property of heterogeneous networks: the network is resilient to the removal of some random nodes, but it fails quickly if the removed nodes share some specific characteristics, thus leading to a subsequent cascade of failures in other nodes.

Here, the dynamics, the exchange of some physical quantities between nodes, plays a much more destructive role in failures than structure topology alone. In the following, a simple model of cascade-based attacks is shown, where the **betweenness centrality** is used as a proxy for the physical quantity exchanged, as proposed in [13]. Among the different measures of centrality, the betweenness easily reproduces the flow of information between any pair of nodes through the shortest path connecting them and is here intended as the load L_j that each node handles at a specific time interval. For each node in the network, the model defines a capacity, that is, the maximum load that a node can handle at a given time. The capacity C_j is set for each node of the network at the beginning of the simulation as in the following

$$C_i = (1+\alpha)L_j \quad j = 1, \dots, N \tag{1.1}$$

where the control parameter $\alpha \geq 0$ is the tolerance of the node. If at a certain time step the load on a node is greater than its capacity $L_j > C_j$, the node fails and an instantaneous rebalancing of the loads is triggered at the next time step. Depending on the way the first node to fail is chosen, cascade failures might be triggered in the network, leading many other nodes to fail and sometime a partitioning of the network in different connected components. Failures propagate in the network as long as the failure conditions are met for any node. The entity of the damage is assessed by the ratio between the sizes of the largest connected components at the end N' and before N the cascade failures happened:

$$G = \frac{N'}{N}$$

1.2 | Cascades on synthetic networks topologies

The effects of cascade failures are tested on multiple undirected unweighted network topologies to compare their resilience against targeted attacks at different values of the control parameter α. To fully test the model, different attack protocols are implemented: Targeted attacks triggered on the node with highest betweenness centrality or with the highest degree, and random attacks triggered sampling uniformly on nodes of the network. The damage caused by the cascade is computed by averaging different independent realizations of the same network topology in order to provide meaningful ranges for the parameter G. Notice that the beweenness-targeted attacks are always triggered on the node with highest betweenness centrality, whereas the degree-targeted attacks add an additional stochastic factor as only one of the 10 nodes with highest degree is used as a trigger for the attacks. These attack protocols require complete knowledge of the network structure, while random attacks sample the trigger uniformly.

Molloy-Reed configuration model is the first network topology tested. Each network is sampled from the ensable where the degree distribution is set to follow the power law:

$$P(k) \propto k^{-\gamma} \tag{1.2}$$

where the exponent γ is varied in the range for the values of $\gamma \in \{2.5, 2.8, 3, 3.1\}$. Each network is made of $N = 1000$ nodes and the minimum degree is set to be 2. The average degree varies depending on the exponent γ, as shown in Figure 5.1(b). In Figure 5.1(a) the different behaviors of the configuration model network are shown, which are strictly influenced by γ. For all the values of γ tested, there are consistent trends in the observable G. It is interesting to note how different attack protocols influence the portion of failed network for different tolerance values α.

Barabasi-Albert model is also tested under similar conditions. The generated networks have all $N = 1000$ nodes, and the only parameter left to vary is the number of edges m added at each time step. The degree distribution is expected to follow the power law $P \propto k^{-\gamma}$ with $\gamma = 3$, the average degree is like $\langle k \rangle = 2m$, and linear preferential attachment is used. As is possible to note in Figure 5.2(b), higher values of m correspond to more abrupt changes in G: for a $\alpha = 0.5$ and a betweenness-based attack protocol, less than 75% of the network is still connected in a single cluster.

Erdős Rényi Gilbert model is tested with varying wiring probabilities p, which in turn depend on the network size N kept constant at $N = 1000$ nodes. The different probabilities range from the critical value $p_c = 1/N$ to $p \propto C \log N/N$, $C > 1$ to get an almost surely connected giant connected component. As shown in Figure 5.1(c), the critical values for α above which cascade failures do not significantly perturb the network are found in the range $0.05 < \alpha < 0.1$. However, only for p so that there is almost surely a giant connected component, critical values for α can be found.

Other models are tested with the same number of nodes N, but with different generating mechanisms. These networks are sampled from the regular lattice ensable with the degree of each node k_j fixed at a certain value, from the Watts-Strogatz ensable

for different rewiring probabilities p_r, and finally from the stochastic block model. The associated graphs are found in the additional material section.

1.3 | Cascade on empirical networks

Cascade-based attacks are of particular interest when they can be mapped to real-world networks such as the Internet and power grids. These theoretical analyses can be used to assess the robust-yet-fragile nature of the networks in order to prevent and mitigate possible attacks to the infrastructures. Their highly heterogeneous distribution of loads makes them vulnerable to targeted attacks on a single node, which in turn can lead to a significant fraction of the network being put offline.

Internet Autonomous Systems - We tested the Internet Autonomous Systems [1], an undirected network of $N = 6474$ nodes, representing routers exchanging information. The average degree is $\langle k \rangle \pm \sigma_k = 4.3 \pm 25$ and the degree distribution is shown in Figure 5.3(b) where the expected power laws for $\gamma = \{2, 3\}$ are drawn for comparison. To characterize the network, in Figure 5.3(a) is shown the betweennees distribution, which at the first stage corresponds to the initial load of the nodes. There is a strong correlation between degree and betweenness, as can be shown in Figure 5.3(c) and for this reason the attack protocol based on degree yields the same results as betweenness-based if no randomness is added to the first attacked node, as the cascade is a deterministic process once it has started. Figure 5.3(e) clearly shows at different values of α the response of the Internet network. It should be noted that even for values of $\alpha = 1$, if the node with the highest betweenness fails, more than 10% of the nodes will also fail due to load rebalancing. On the contrary, degree-based attacks are not as effective and the sudden drop in the region $\alpha \sim 0.2$ can be explained by chance when computing the averages on the network. In fact, the G ratio is expected to grow constantly with higher values of α. As expected, random attacks are efficient only in the very low α regime and are not yet as effective as the other protocols. Figure 5.4(e) finally shows the status of the network at the end of the cascade failure triggered by the highest betweenness node, higlighting the largest connected component.

Western US Power Grid - An analogous analysis is performed on the Western US Power Grid network [2], made up of $N = 4941$ nodes representing transforms or power relay points, and two nodes are connected if a power line runs between them. This network corresponds perfectly with the model simulated, as the rebalancing of the loads is almost instantaneous and the current can travel in both ways of each edge, being the network undirected also in the real life scenario. Following the procedures described above, the resilience of the network is assessed and in Figure 5.3(d) the distances from the first and second nodes to fail are reported, compared to the distances from the first node to fail and any other node in the network. The histogram shows the non-local effects of the cascade, that is, the second failing nodes do not necessarily need to be direct neighbors where the distance is 1. At the same time, the second failing nodes are not further than 9 edges, while the furthest node is 27 edges away, as shown in the histogram.

2 | Self-Organized Criticality

Task leader(s): *Guglielmo Bordin, Alessio Pitteri*

2.1 | The sandpile model

In this task, we will study the dynamics of the so-called *sandpile model* – first described in a 1987 paper by Bak, Tang, and Wiesenfeld (Bak-Tang-Wiesenfeld or BTW sandpile model) [5]. We will apply this model to different types of synthetic and real networks. The purpose of the model is to simulate the response of a graph to a slow external driving, represented by the constant addition of a discrete *load* to each node. These load units are commonly referred to as "sand grains", which inspired the model's name.

The algorithm is straightforward: at each time step, a grain is added to a random node i; then, the current load level in the node is checked against a predefined threshold C_i, the *capacity* of the node. If the load equals or exceeds the threshold, the node *topples*, and all the sand grains are transferred to its neighbours. This marks the start of an *avalanche* event. In this work, we choose the degree k_i of the node as the threshold, as it is common in the literature [6, 7, 12]. Additionally, this approach aligns well with real situations of loaded networks, such as power grids, where more connected nodes are likely to be more reinforced [7]. After the first load redistribution, the level in the neighbouring nodes is checked against their thresholds, and if the toppling condition is met in any of them, the avalanche continues, redistributing grains to the neighbours until every node in the network returns to a non-critical load level. The addition of new grains is halted during an avalanche; that is, the relaxation process is considered to be very fast compared to the external driving time. Also, to add an "escape valve" to the system and allow it to dissipate grains, we define, following [12], a *sink fraction* f, which represents the probability to drop a grain during a load transfer. Unless stated otherwise, we will use a sink fraction of 0.01 throughout the analysis.

The most interesting feature of the sandpile model is the concept known as "self-organized criticality". The idea is that the system has a critical state that is robustly reached without the fine-tuning of any external parameter, unlike in the phase transitions of classical statistical mechanics, where the system needs to be in a restricted region of the phase space to achieve critical behaviour. Thus, the criticality is said to be self-organized in the sense that the system reorganizes itself to reach a state characterized by many hallmarks of criticality, chiefly scale invariance manifested through a power-law distribution of the avalanche sizes.

2.2 | Avalanche size distribution

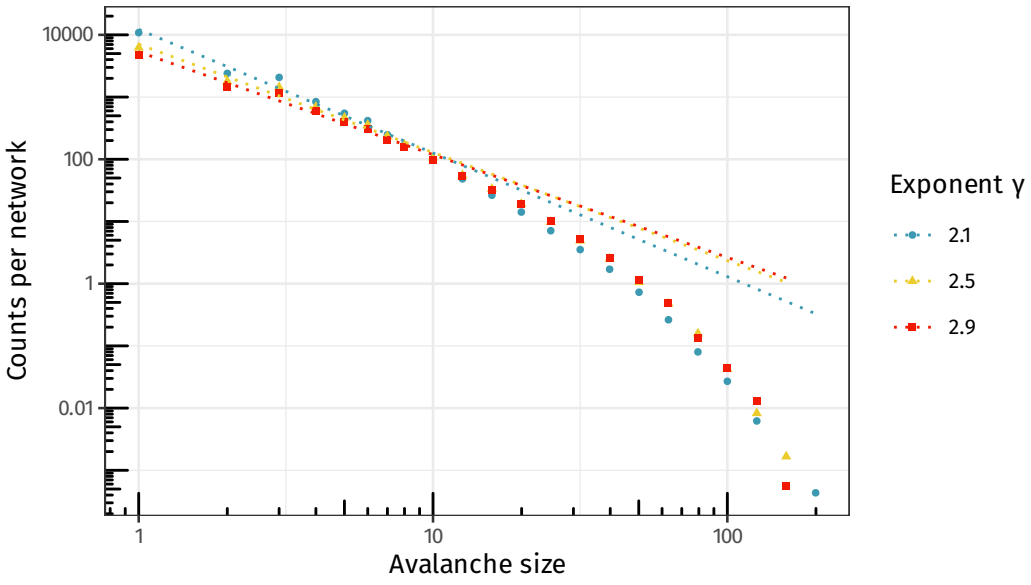


Figure 2.1: avalanche size distribution from simulated scale-free networks with three different γ exponents. n was set to 10 000 and m to 20 000 before generating each network; then, only the largest connected component was selected. The final data is averaged over 50 replicas for each γ and logarithmically binned. The results of linear fits performed on the sizes smaller than 12 are displayed with dashed lines.

We define the *size* of an avalanche s as the total number of toppling events that it comprises. Another related quantity is the *area* a, defined as the number of involved nodes, i.e. each toppled node is counted once [12]. Other relevant quantities are the *duration* t, the number of parallel topples before the avalanche stops, and the number of toppled grains w. We should point out that, for the following calculations, we considered only the so-called *bulk* avalanches, i.e. the avalanches without any loss of grains (we refer to the supplementary materials section for the motivation behind this choice).

We know from the literature, both from previous numerical simulations [5, 6, 12] and from a mean-field theory derived from viewing the self-organized critical state as a critical branching process [3], that the avalanche sizes in the critical phase distribute as a power law with an exponential cut-off: $P(s) \sim s^{-\tau} e^{-s/s_c}$.

Goh, Lee, Kang and Kim [12] extended the branching process theory approach to derive a mean field exponent for $P(s)$ in the case of scale-free networks with a degree-distribution exponent γ between 2 and 3. The mean field τ scales as $\gamma/(\gamma-1)$. To check this result, we conducted simulations on several scale-free networks with different γ exponents, which were generated using the static model [11]. Once the bulk avalanches in the critical state were selected, we logarithmically binned the size distributions and performed a linear fit on the points before the exponential dip in the log-log plot. The results are summarized in Tab. 2.1; we found a reasonably good agreement, with a bit more discrepancy for $\gamma > 2.5$.

γ	τ_{mf}	τ_{fit}	95 % CI	p-value
2.1	1.91	2.0(1)	[1.70, 2.28]	0.73
2.3	1.77	1.8(1)	[1.56, 2.05]	0.64
2.5	1.67	1.7(1)	[1.51, 1.97]	0.77
2.7	1.59	1.7(1)	[1.47, 1.90]	0.84
2.9	1.53	1.7(1)	[1.44, 1.86]	0.90

Table 2.1: fitted values of the avalanche size power law exponent and comparison with the mean-field value $\tau_{\text{mf}} = \gamma/(\gamma - 1)$.

2.3 | Western US Power Grid

Having verified the general behaviour of the avalanche size distribution in a synthetic scale-free network, we investigated the dynamics on a real network, comparing it to its null model. The network we have chosen is the already mentioned Western US Power Grid. Its degree distribution has a power-law tail with exponent approximately 3.3, but with relatively few leaves. We constructed a set of replicas of null-networks with the same degree sequence through a configurational model, and tested the power grid network's diameter, global clustering coefficient and power-law exponent of the size distribution against the null hypothesis.

The two structural observables, diameter and clustering, are remarkably different in the real network ($D_{\text{pg}} = 46$ against a mean $D_{\text{null}} = 23(2)$, and $C_{\text{pg}} = 0.1$ against a mean $C_{\text{null}} = 7(3) \times 10^{-4}$). Perhaps unsurprisingly, we found a strong contrast also in the avalanche size exponent τ, with $\tau_{\text{pg}} = -0.98(5)$ against $\tau_{\text{null}} = -1.09(2)$, 6 standard deviations from the mean of the null distribution. This means that small avalanches are (slightly) less probable and medium-sized ones slightly more. For the huge avalanches, the exponential cut-off is dominant, so we cannot say anything on the matter having fitted the linear part of the distributions.

2.4 | Total load capacity

We define the effective capacity η as the fraction of the maximum number of grains that a system can support, divided by the total theoretical capacity $\sum_{i=1}^{N}(k_i - 1)$. This value is, of course, always lower than 1 due to probabilistic and structural reasons.

We observed that after a certain threshold number of grains, the system stabilized, reaching an equilibrium η. This quantity could be interpreted as the maximum load that a real power grid can support. Therefore, we are now interested in studying the behaviour of η as a function of the number of edges (i.e., the number of cables) for different types of models with a fixed number of nodes. The results are summarized in Fig. 2.2.

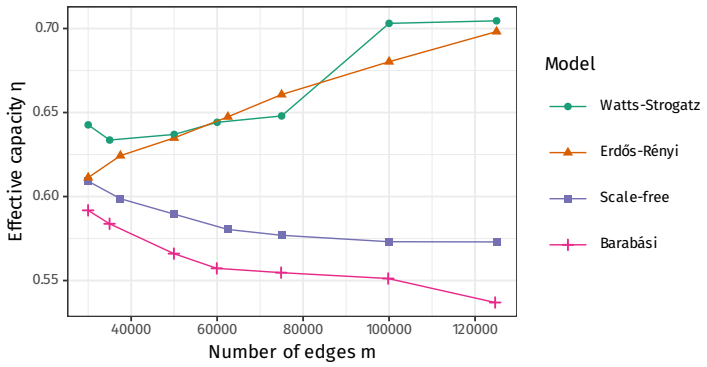


Figure 2.2: comparison of the effective capacity as a function of the number of edges, for different kinds of synthetic networks (Watts-Strogatz small-world model, Erdős-Rényi model, scale-free with $\gamma = 2.5$ and Barabási). All networks have 5000 nodes, and the parameters are adjusted to get the corresponding m values on the x axis.

3 | Traffic congestion

Task leader(s): *Davide Bacilieri, Maximilian Matzler*

3.1 | Introduction

In this chapter, we will explore the phenomenon of traffic congestion. In a nutshell, our model is a network to which we add a temporal dynamics consisting of the creation of new packets within each time step along with their motion between randomly chosen nodes, vanishing from the network as soon as they reach their pre-determined destination.
We will simulate this process on empirical as well as synthetic networks, which are created via a modified Barabasi-Albert procedure. The usual BA procedure consists of gradually creating a network by adding a new node at each time step with a constant number m of (outgoing) edges. These edges get connected to existing nodes with probability $P \propto k_i$, where k_i is the number of edges connected to the (existing) node i, also called degree.
Such networks are also called scale-free, because their degree distribution follows a power law

$$P_k \propto k^{-\gamma} \tag{3.1}$$

with γ being constant.
Our modification consists of initially creating a small network of size m_0 according to the usual BA procedure and assigning each node i a random number between 0 and 1, dubbed affinity or a_i. For each newly added node j, we also create an affinity and only allow its outgoing edges to connect to nodes i fulfilling $a_i \in (a_j \pm \mu)$, where μ is the tolerance, a constant between 0 and 1. Conceptually, this accounts for some form of spatial vicinity, since nodes with similar affinity tend to have more connections among themselves.
The traffic on the network is modelled as follows: for each time step, in each node a packet is generated with probability p/N, with destinations randomly chosen among all the nodes in the network. Also, at each time step each packet in the network moves to one of the neighboring nodes, vanishing as soon as it reaches its destination node. Every node can only handle one packet per time step, which leads to packets queuing in nodes. We implement the following delivery strategy: packets choose their next node i according to the shortest effective distance

$$d^i_{\text{eff}} = h\, d_i + (1-h)\, c_i \tag{3.2}$$

where d_i is the shortest path between node i and the packet's destination, c_i the length of queuing processes at node i, and h is a parameter called *traffic awareness*. We call the case $h = 1$ the *standard protocol*, where there is no traffic awareness and the nodes are only chosen w.r.t. shortest physical distance.

3.2 | Phase transition for a synthetic vs. an empirical network

Ref. [9] predicts a phase transition between a free flowing phase of the system, where an equilibrium between the number of created and delivered packets develops, and a congested phase, were the number of packets in the system increases until in the most extreme case there is no packet delivery at all.
The phase transition can be visualised by considering the order parameter

$$\rho = \lim_{t->\infty} \frac{A(t+\tau) - A(t)}{\tau p} \tag{3.3}$$

with τ observation time and ρ ratio between outflow and inflow during time window τ. The authors of Ref. [9] show that while $h = 1$ triggers a second-order like phase transition, $h \neq 1$ leads to a first-order like phase transition, which occurs at a higher critical value ρ_c, but with an abrupt jump in the value of the order parameter.
In Fig. 7.2, the order parameter ρ is averaged over several runs for several different values of p to demonstrate the phase transitions. The modified BA network used in these simulations had a total number of 500 nodes and a tolerance of $\mu = 0.243$. In the left plot, the qualitative difference between the two phase transitions as well as the difference in the transition point can be distinguished well. For the empirical network on the right hand side, the jump is not abrupt, as for the synthetic network, but there is a qualitative difference in the curve: For $h = 0.82$, the slope is first concave upwards and then concave downwards, as opposed to the case $h = 1$.

3.3 | Further analyses

We will now take a closer look on the influence of the parameter h on the performance of the network. In order to do that, we plot the number of active packets $A(t)$ against time t for different values of h and p.
[10] proposes a further modification made to the packet delivery algorithm labelled *stochastic protocol*, which we shall briefly discuss: Instead of choosing the neighbor to which a packet gets delivered deterministically, we define a score or energy function $H_i = h\, d_i + (1-h)\, c_i$ with h, d_i and c_i as above. Moves are not chosen by selecting the neighbor with minimum H_i, but sampling from all neighbors with respective probabilities

$$\Pi_i \propto \exp(-\beta H_i), \tag{3.4}$$

where β is a tunable parameter corresponding to an "inverse temperature". Let us evaluate the influence of β on the number of active particles $A(t)$:

As evident from Fig. 7.4, values of β introducing randomness into the choice of neighbor decrease the performance ($\beta = 2$), while higher values suppressing higher effective path lengths lead to similar results as the deterministic approach.

The influence of the traffic awareness h onto the number of active particles $A(t)$ shall also be discussed: In the first row of Fig. 7.6 one can see how the transition point for the traffic-unaware protocol ($h = 1$) is being crossed, while varying values of $h < 1$

still handle the traffic. In the middle of the second row, the plot for $p = 15$ zooms in (one can see $h = 1$ leaving the picture very early) to show that higher values of $h < 1$ achieve a slightly better performance by keeping the number of active packets lower. In the last plot ($h = 20$) we can see that the transition point has also been crossed for $h = 0.1$ and $h = 0.3$, and the accumulation of packets is even more rapid than in the case $h = 1$.

3.4 | Results for real networks

Next, we try to reproduce the phase transition between to the congested regime for a real, empirical network. We use the internet autonomous system network [1], which is also used in task 1, where a discussion of its properties can be found.

In this case, the transition for h<1 is more gradual, taking the shape of a generic sigmoid function, as seen in Fig. 7.2

3.5 | Comparison to analytic solution

Lastly, we perform a further version of the traffic routing protocol on another different topology, namely a hierarchical tree. We compare the obtained results to an analytical solution existing for the specific scenario, as demonstrated in Ref. [4].
A hierarchical tree is constructed level by level by starting with one node, adding z nodes connected to the initial node, then connecting z further new nodes to each of these nodes, and so on. Subsequently, the network is fully defined by the pair of numbers (m, z), where m represents the number of levels.
The degree distribution of this network is trivial, as is the betweenness, with equal betweenness among nodes of a layer and the betweenness rising, the closer one gets to the central node (see supplementary material for plot).
The routing of packets is modified here insofar, that we define quality of communication of between nodes i and j according to

$$q_{ij} = \frac{1}{\sqrt{n_i n_j}}, \tag{3.5}$$

where n_k describes the number of particles currently at node k. It is worth mentioning that in this model, there is no queuing: each packet has its own probability of jumping to the next node. Ref. [4] analytically determines a transition point (independent of network size at

$$p_c = \frac{\sqrt{(z)}}{\frac{(z(z^{m-1}-1)^2}{z^m-1} + 1}. \tag{3.6}$$

Note that p_c here is the creation probability of a new packet at any given node.
Here, we analyse such a hierarchical tree with $(z, m) = (5, 3)$, which corresponds to $p_c = 0.0923$, or $P_c = N\,p_c = 14.399$.
While the qualitative behavior reminds of the phase transitions observed earlier, the quantitative transition point cannot be reproduced: in our realisation, it lies between 2.5 and 2.75, which is far off the predicted value of 14.399.

4 | Complex Contagion

Task leader(s): *Marco Zenari*

4.1 | Introduction, model motivation and specification

In this task we will study how a small initial shock can cause a cascade failure in a large complex system. We do that by simulating the phenomenon in sparse random networks of interacting agents that influence the decisions of the others according to a simple threshold rule, as done in Ref. [16]. A peculiar property of this phenomenon is that the very same systems show stability under small failures and suddenly show a cascade failure caused by a particular shock. This is an example of the *robust yet fragile* nature of many complex systems [8]. We develop a simple model with the intent of studying a population of individuals who must decide between two alternative actions and they rely on the decision of other members of the population. This type of dynamics is known in economy as *Binary Decisions with Externalities* (Ref. [15]) and happens when decision makers have limited information about the problem or are unable to process the information they have. The decision can be considered as a function of the relative number of other agents who are observed to choose one of the two alternatives. This type of decision has an intrinsic threshold nature, due to the cost and commitment of resources that it implies. Decision makers are modeled as nodes of a network that can be in two states: either 0 or 1. They interact with k other agents which are the nodes to which they are connected and represent the signals that an agent receives. All nodes start in state 0 and, after that some of them are randomly or targetly chosen to be set to state 1, the evolution of the network consists in changing the state of a node from 0 to 1 if the fraction of its neighbors in state 1 is higher than its threshold Φ. When a node reaches state 1, it maintains it for the rest of the evolution. Every node is assigned a threshold Φ drawn at random from a distribution $f(\Phi)$ such that $\int_0^1 f(\Phi)d\Phi = 1$. We can define the *seeds* as the nodes that are initially set at 1 and the *vulnerable* nodes as the nodes that, based on their threshold Φ, would change state if just one of their neighbors k is set to 1, meaning if $k \leq \lfloor 1/\Phi \rfloor$. The nodes that are not vulnerable are called *stable*. In the language of the diffusion of innovations the initial seeds play the role of the *innovators* and the vulnerable nodes play the role of the *early adopters*.

4.2 | Exact solution on random graphs

In this section we try to find an analytical solution to the problem of understanding when the cascade occurs in a random network. We consider for the calculation undirected random graphs with a specified degree distribution p_k and $z \ll n$, where z is the average degree of a node and n is the number of nodes (real networks in general

tend to be very sparse). We define *globally cascade* a cascade in which the interested fraction of nodes that reach the state 1 is finite in an infinite network. In a sufficiently large graph with a seed sufficiently small, no vertex neighboring the initial seed will be adjacent to more than one seed. This is in particular true if we choose only one node as the initial seed. Under this condition, the only way a seed can grow is if at least one of its immediate neighbors is a vulnerable node. Therefore we conjecture, and this is the main hypothesis for our calculation, that for having a global cascade the subnetwork of vulnerable nodes must percolate. We can translate this statement in mathematical constraint using a generating function approach (full derivation exploited in the supplemental material 8.1). Suppose that every node has a degree k with probability p_k and that a node with degree k is vulnerable with probability ρ_k, than the *cascade condition* is given by:

$$\sum_k k(k-1)p_k\rho_k = z. \tag{4.1}$$

In particular, if the left hand side of equation 4.1 is less than z the early adopters are isolated from each other and will be unable to generate the momentum necessary for a global cascade. Vice versa if the LHS of 4.1 is greater than z the vulnerable cluster percolates the network. Note also that equation 4.1 is monotonically increasing in k but ρ_k is monotonically decreasing, suggesting that there will be two solutions, corresponding to two phase transitions and a window of values of z for which we expect global cascades to occur.

4.3 | Simulations with Erdős Rényi Gilbert model

In this section, we illustrate the first set of simulations that we have implemented on Erdős Rényi Gilbert networks, e.g. uniform random graph in which each pair of nodes is connected with probability $p = z/n$ where z is the average degree and n is the number of nodes. In particular, we sample networks with $n = 10000$ nodes and each node has the same threshold Φ^*, meaning $f(\Phi) = \delta(\Phi - \Phi^*)$. For this type of networks, the cascade condition 4.1 reduces to equation $zQ(\lfloor 1/\Phi \rfloor - 1, z) = 1$ where $Q(a, x)$ is the incomplete gamma function. This condition can be solved with numerical methods to obtain a prediction of the cascade window: the upper incomplete gamma function will give the upper bound of the window, while the lower incomplete gamma function will give the lower bound. For the simulations, we have explored the (Φ, z) phase space and observed if the global cascade would have occurred in 25 realization of the network. The results are shown in Fig. 4.1 (a) and the comparison with the theoretical prediction is not as accurate as expected. This is due mainly to two factors: in the simulation we are working with finite networks and we have tried only 25 realizations of the same parameters. It is possible that with more realization we would have found a seed that would have triggered the cascade. In Fig. 4.1 (b) we observe the evolution time of each network varying z and keeping fixed $\Phi = 0.18$, with 100 realizations for each case. It is evident that there are two phase transitions: one at $z \simeq 1$ and the other at $z \simeq 6$. In Fig. 4.1 (c) is shown that the fraction of nodes involved in the cascade is compatible with the size of the largest connected component which has been evaluated by solving numerically the theoretical self-consistency equation $S = 1 - e^{-zS}$ (Ref.[14]). In Fig. 4.1 (d) is compared the empirical probability of triggering a global cascade (from simulations) with the size of the vulnerable connected component and

the size of the extended vulnerable connected component that are obtained as mean of 100 realizations of the networks. The second appears to fit the data better because it takes in to account the nodes that are adjacent to the vulnerable cluster, which, even though being stables, can trigger the cascade because neighbors of vulnerable nodes. Picking an initial seed at random will trigger the global cascade if the node belongs to the extended vulnerable cluster. Other simulations that investigate the behavior of global cascades under heterogeneous thresholds and different network models such as Barabasi-Albert are reported in the supplementary material 8.2, 8.3.

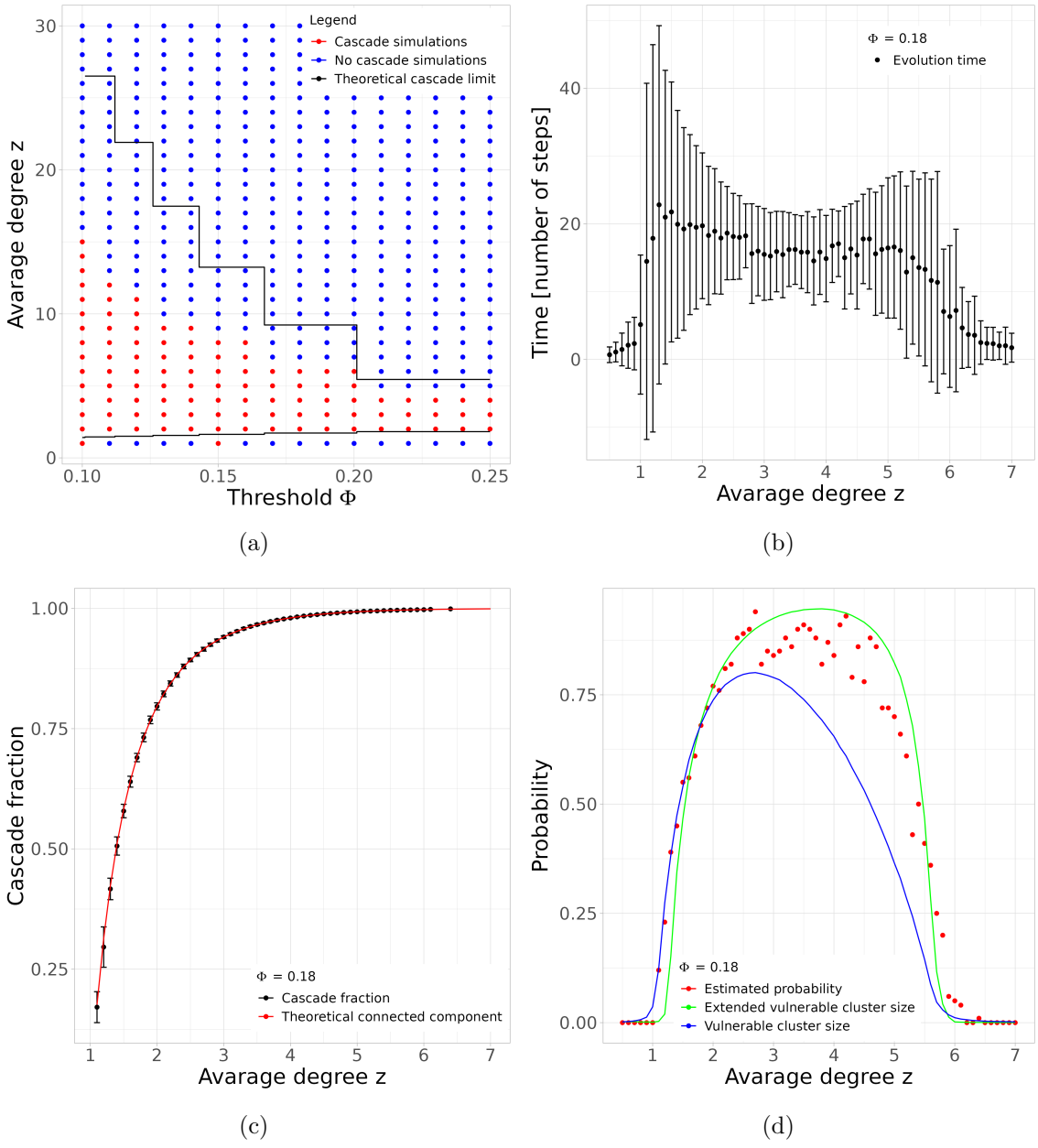


Figure 4.1: Simulations for Erdős Rényi Gilbert networks in the threshold model. (a) Cascade window analyzed in the phase space (Φ, z) with comparison between simulations and theoretical prediction. (b) Evolution time of the dynamic fixed the threshold $\Phi = 0.18$ and varying the average degree z. (c) Comparison between cascade fraction and largest connected component size (same parameters as (b)). (d) Probability of triggering a global cascade and comparison with vulnerable and extended vulnerable clusters sizes (same parameters as (b)).

5 | Supplementary material - Motter-Lai model

Task leader(s): *Tommaso Bertola*

5.1 | Cascades on synthetic networks topologies

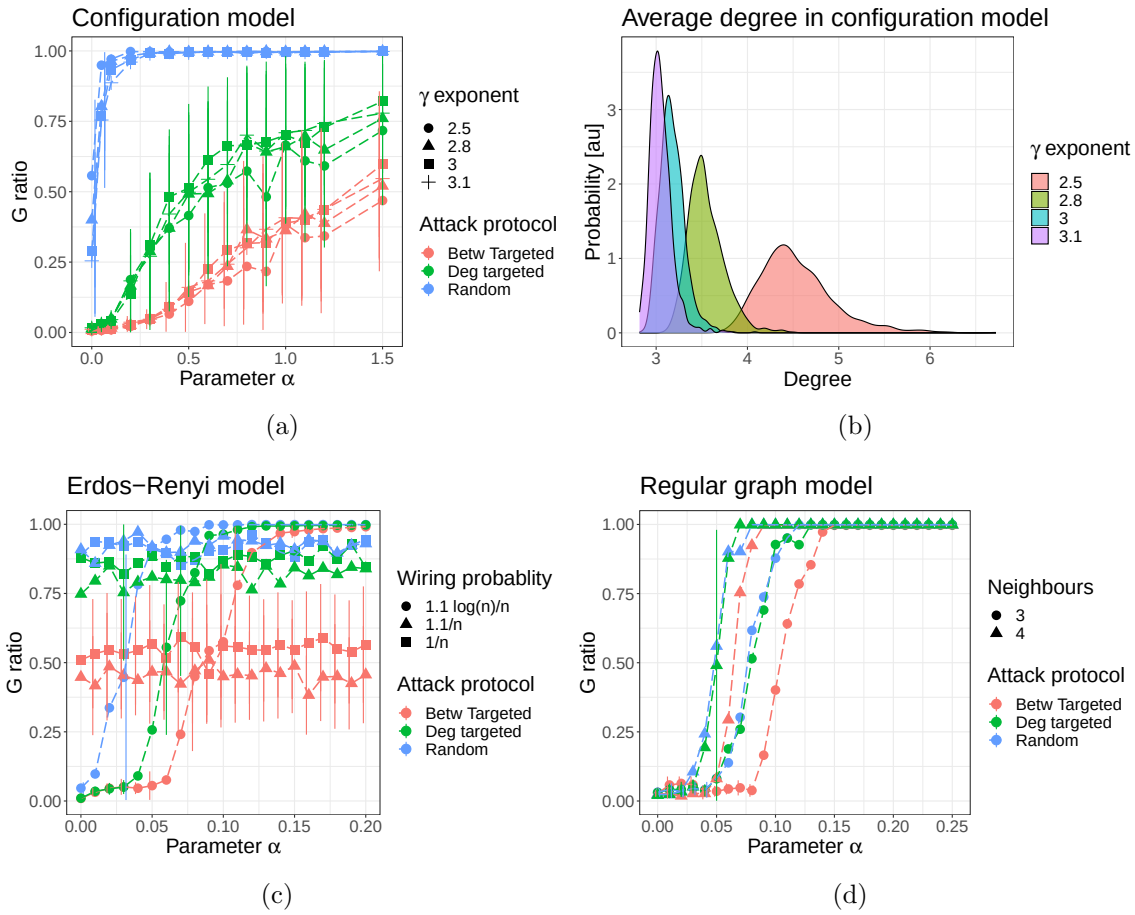


Figure 5.1: (a) Behaviour of Molloy-Reed configuration model under different attack protocols and different γ exponent in number of edges generated (b) How the average degree in configuration model networks depends on the γ exponent (c) Erdős Rényi Gilbert network response at different wiring probabilities p, for $p \propto 1/n$ where $|\text{LCC}| \sim N^{2/3}$, $p \propto C/N\, C > 1$ where $|\text{LCC}| \sim N$ and $p \propto C \log N/N\, C > 1$ where the GCC is surely connected. For the highest p, a sharp phase transition is observed for $\alpha \sim 0.05$ (d) Attack response for a regular lattice with varying number of neighbours

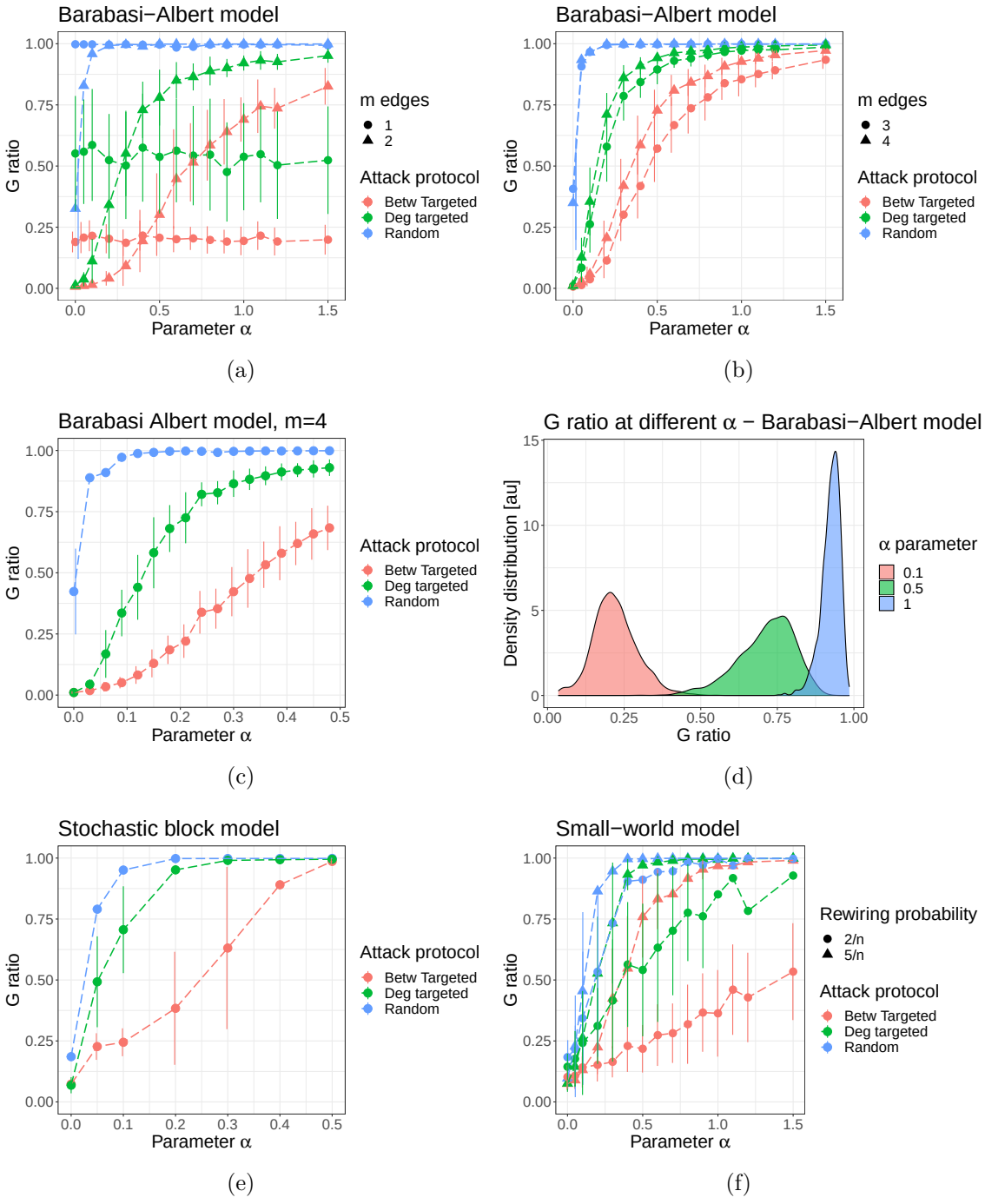


Figure 5.2: (a) Barabasi-Albert linear preferential attachment response. Only for $m \geq 2$ a phase transition in the resilience of the network is found (b) Barabasi-Albert for higher m. Steeper phase transition for lower values of α are observed (c) Focus on different attack protocols for Barabasi-Albert $m = 4$. At $\alpha = 0.5$ less than 75% of the network is still in the largest connected component or not failed (d) How different α influence the response of the Barabasi-Albert network response in the limit of many independent realizations (e) Stochastic block model for a single realization on a network of 8 distinct clusters, check source code for more insight into the network topology (f) Small-world response at different values of the rewiring probability

5.2 | Cascade on empirical networks

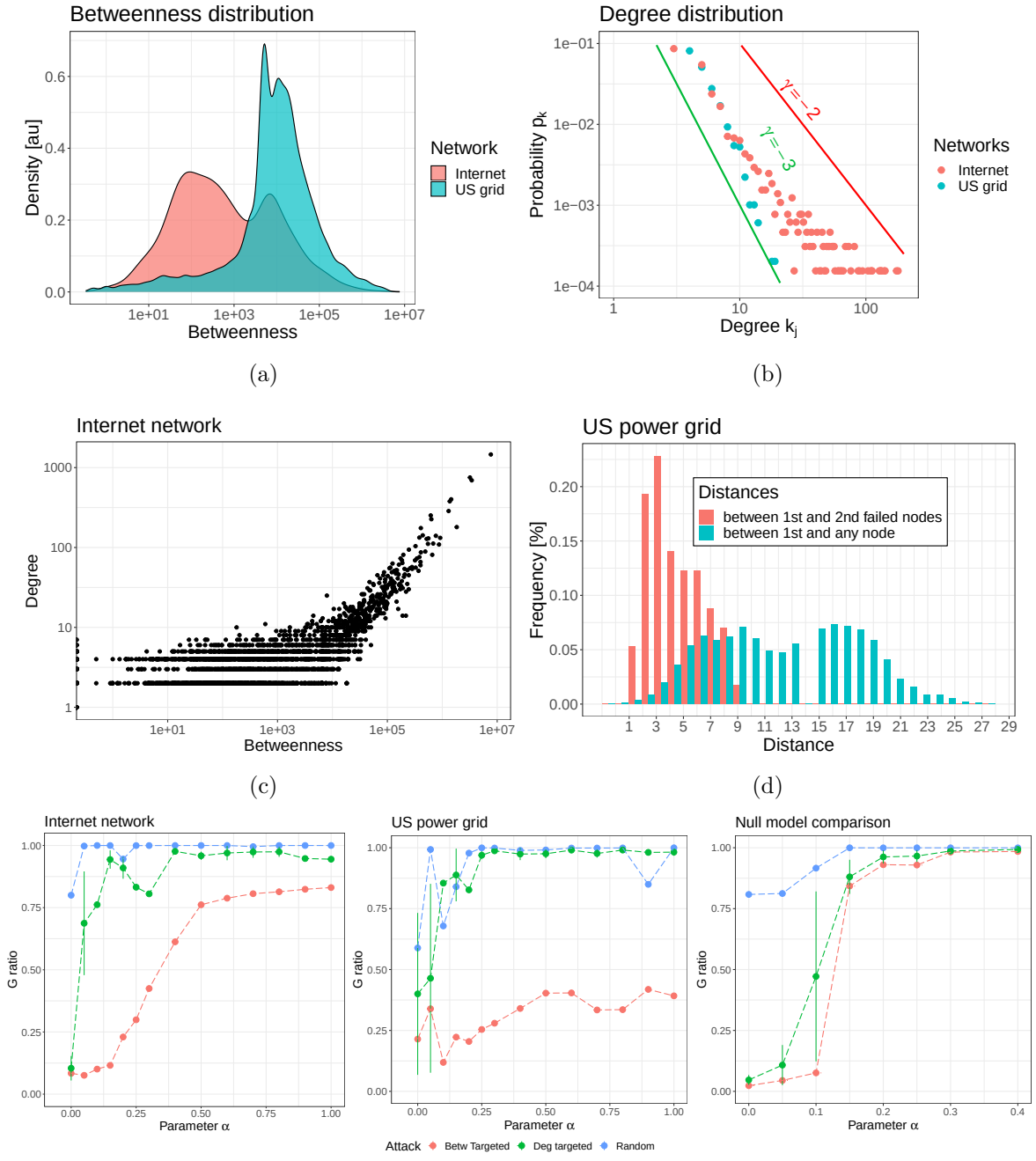


Figure 5.3: (a) Betweenness centrality distribution for the two empirical networks, spanning 7 orders of magnitude (b) Degree distribution in empirical networks. The distribution is typical of a power-law and $y \sim x^{-\gamma}$ for $\gamma = \{2, 3\}$ are drawn for comparison. (c) Correlation between degree and betweenness centrality. Nodes with higher degree tend to have higher betweenness centrality. (d) Nonlocal effects in the failures: in red are shown the distances from the first node to fail and all the nodes to fail as a consequence. More than half of the second nodes to fail are more than 4 hops apart from the triggering failure. In blue are shown all the distances from the first node to fail to all the other nodes. (e) Response of the two networks under analysis. For the US power grid, even $\alpha = 1$ is not enough to prevent more than 50% of the network from failing. (e.right) shows how a null model obtained from the degree sequence of the US power grid responds to the attacks. For values of $\alpha \sim 0.1$ the network is still functioning: the mechanism behind the network topology is relevant to the response to failures.

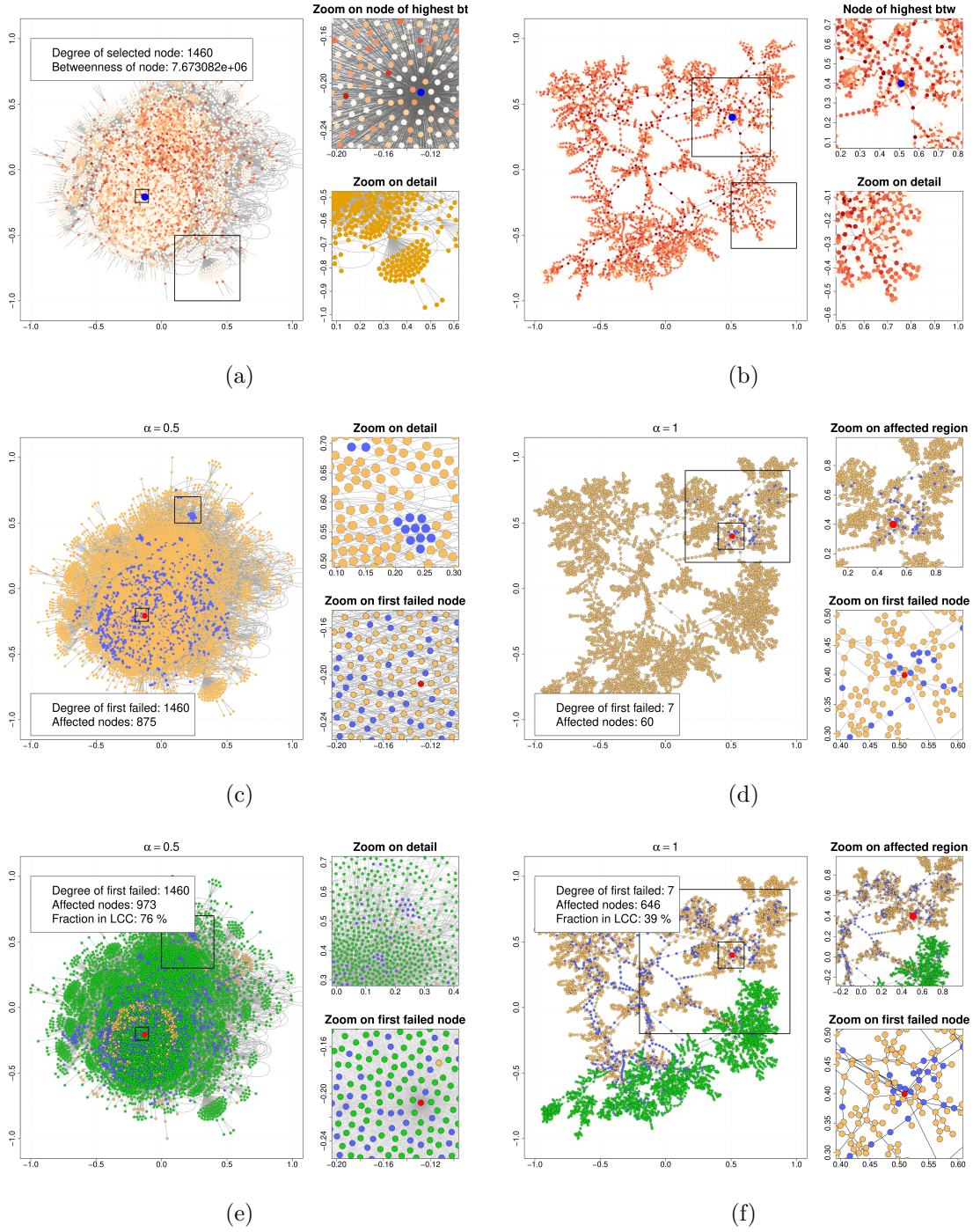


Figure 5.4: Left column is the Internet network, right column is the US power grid network. (a)-(b) Highlight of the network structure. Darker nodes have higher betweennes centrality scores. The blue dot shows the first node to fail under beweenness-based attacks (c)-(d) Shows how the first cascade of failures affects the network. Especially in the Internet network nodes are evenly spread around. The high number of nodes and edges make it difficult to visualize. (e)-(f) In blue are represented all the nodes that failed under the load rebalancing, in green are shown the nodes of the largest connected component at the end of the cascade. In orange are shown all the nodes that did not fail but do not belong to the largest connected component.

6 | Supplementary material – Self-Organized Criticality

Task leader(s): *Guglielmo Bordin, Alessio Pitteri*

6.1 | Clarifications on the critical phase

Concretely, the system first undergoes a transient phase where the load slowly builds up (see Fig. 6.1), with occasional short-lived avalanches. During this initial stage, the sink mechanism is rarely triggered due to the relatively small number of toppling events. To draw a physical analogy, we can say that there is a net influx of energy with little dissipation. After reaching a certain threshold in the total load, large avalanches suddenly appear; these avalanches last long enough to activate the sink mechanism, causing the system to lose grains in a sustained manner. The outgoing flux balances the ingoing flux, resulting in an overall stationary state. As we said, here the avalanches have no typical size or duration: depending on the node where they originate, they can last a few cycles or grow to encompass the entire network, waiting for the sink to activate and return to a stable configuration.

The stationary state is reached regardless the specifications of the system are. The only tunable parameter is the sink fraction, and we have found that, as long as it stays reasonably low – under 0.1 – all analysed networks were able to reach the self-organized criticality. If the sink fraction is too high, there can be long cycles of oscillations in the total load instead of proper stationarity. However, the amplitude of these oscillations diminishes over time.

Indeed, the original formulation of the sandpile model in the BTW paper [5] pertains to a regular lattice with well-defined boundary nodes that act as sinks. Having a global sinkage probability may not be exactly equivalent, but it is more appropriate for the case of complex networks for which we cannot assign a meaningful "boundary". In any case, it is commonplace in the literature, and when combining low sinkage probability with a large system size, the difference is not expected to be relevant [7].

6.2 | Bulk avalanches

We want to point out the motivations behind the choice of discarding from the analyses the avalanches with any loss of grains. The main advantage of doing so is that we get a much "cleaner" size distribution. In fact, many of the non-bulk avalanches come from situations where the system gets stuck in a completely unstable configuration, where the only way out is to wait for the sink to activate. This kind of avalanches easily grow to encompass the whole network, and often go over it in waves multiple times.

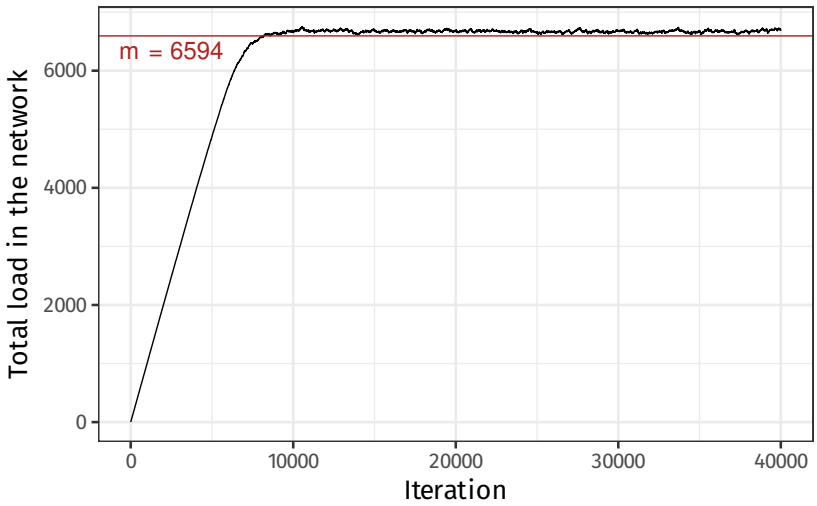


Figure 6.1: evolution of the total load in a typical sandpile simulation. The network used for this simulation is the previously mentioned Western US Power Grid, which consists of 4941 nodes and 6594 edges. In the critical state, the total load is stable around a level close to the number of edges, showing minimal fluctuations.

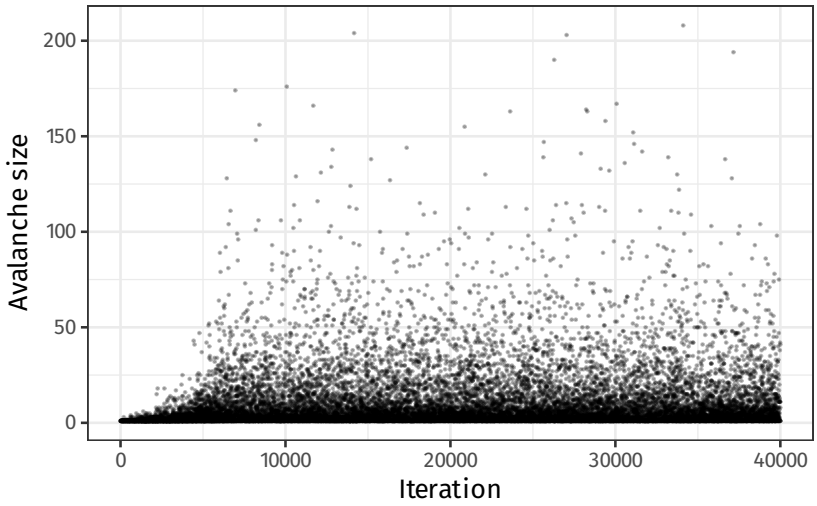


Figure 6.2: (bulk) avalanche sizes in a typical sandpile simulation over the Western US Power Grid. The transition to the SOC regime is evident around the 5000th iteration.

This causes the size distribution to have a visible "quantization" in multiples of the node count, and in turn clutters the tail of $P(s)$ in the log-log plot. Also, regarding what was said in the previous section about the sink mechanism, in keeping only the bulk avalanches we can effectively detach the analysis of the more interesting quantities from the actual implementation of the dissipation mechanism.

In any case, the scale-free distribution of the avalanche sizes is still preserved, being only partially reduced in the higher end of the tail.

7 | Supplementary material - Traffic Congestion

Task leader(s): *Davide Bacilieri, Maximilian Matzler*

7.1 | Graphs

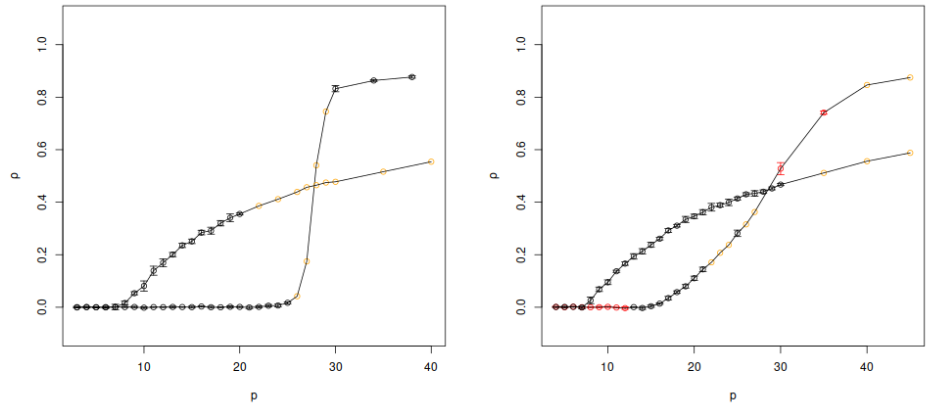


Figure 7.1: Variation of ρ for different values of p in the modified BA model (left) and Internet network (right), with h=1 (leftmost transition point) and h=0.82 (rightmost transition point). Lighter-colored points denote values obtained with less runs.

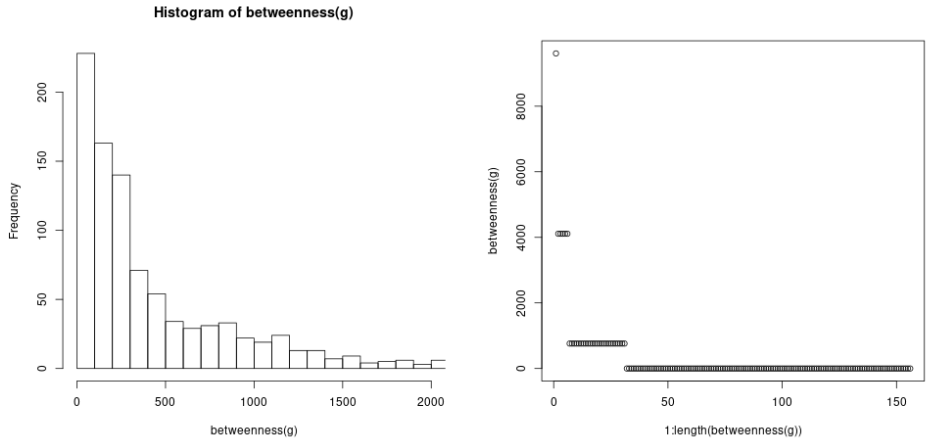


Figure 7.2: Betweenness of the two synthetic networks: On the left hand-side, we put a histogram for the modified BA-procedure, zoomed into the region where the most nodes are located, while on the right hand side one can see all nodes and their betweenness for the hierarchical tree.

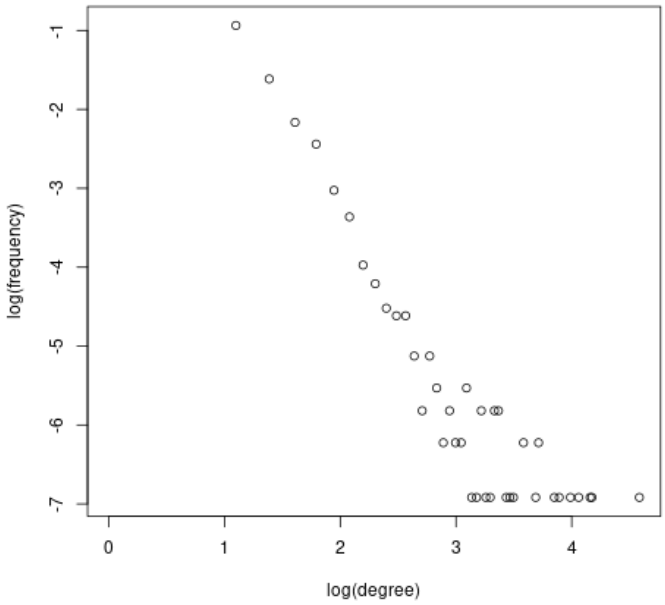


Figure 7.3: Degree distribution of a modified Barabasi-Albert network. The network is created by first building a normal BA network of size $m_0 = 10$ with a number of outgoing connections $m = 3$. The tolerance is set to $\mu = 0.23$ and the total number of nodes $N = 1010$. The qualitatively visible linearity of the log-log plot demonstrates that the degree distribution behaves similar to an ordinary BA network. The degree exponent can be roughly estimated to be 3.067 by fitting a line considering all points in the plot up until the first frequency is zero.

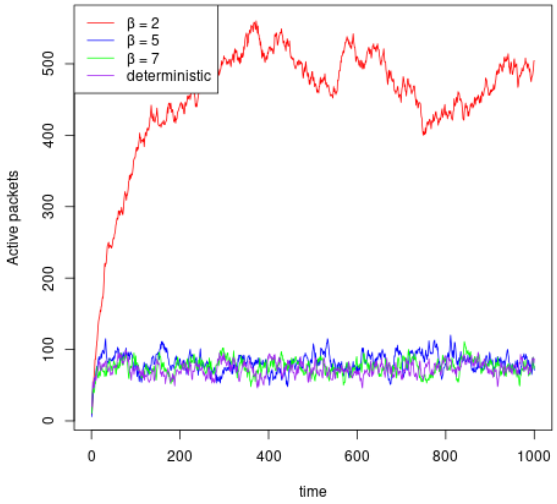


Figure 7.4: Temporal development of the number of active packets for different values of β. The network used is the above-mentioned modified BA graph with a number of nodes $n = 1010$, and a tolerance of $\mu = 0.3$. The traffic awareness was set to $h = 0.82$ and the average number of new nodes was set to $p = 15$, which is slightly under the transition point.

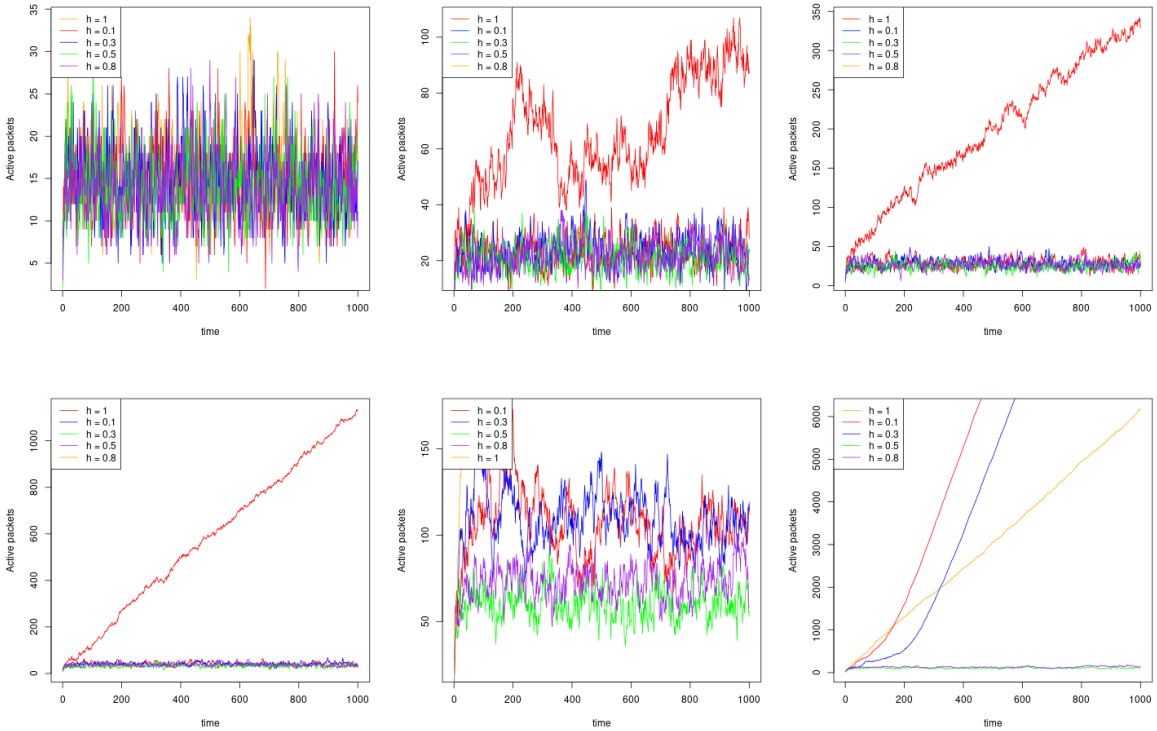


Figure 7.5: Temporal development of the number of active packets for different values of h and $p_i \in (5, 7, 8, 10, 15, 20)$. The network used is the above-mentioned modified BA graph with a number of nodes $n = 1010$, and a tolerance of $\mu = 0.3$.

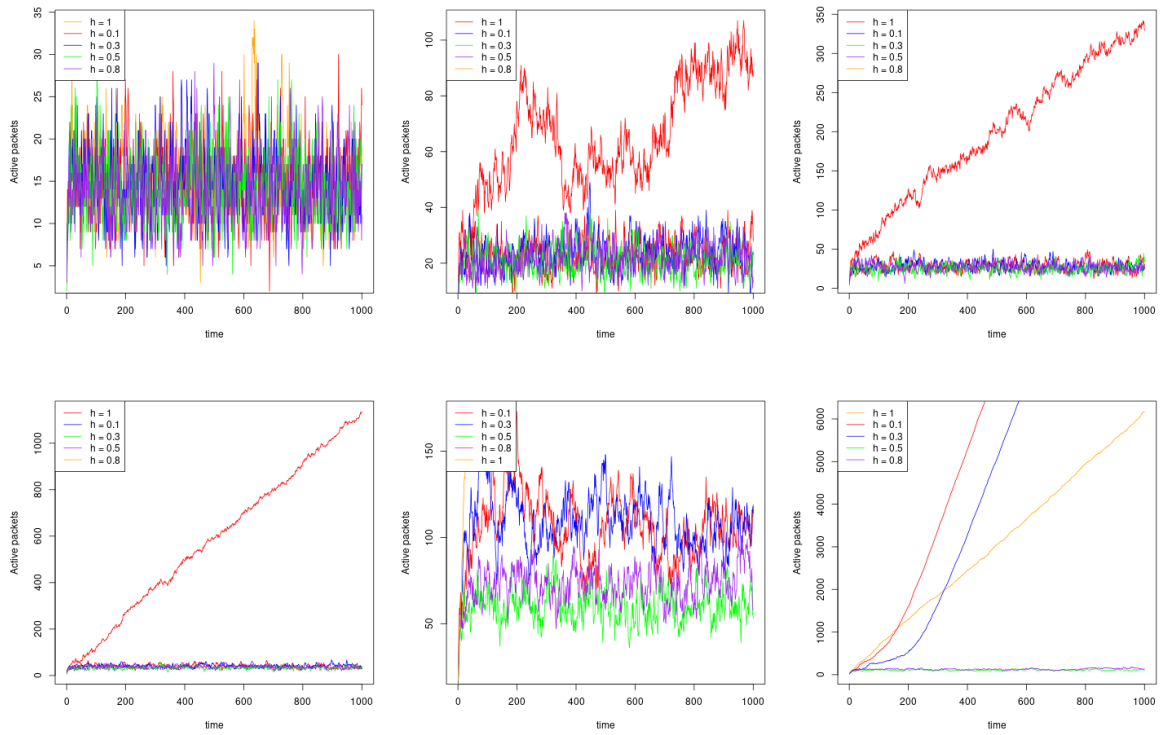


Figure 7.6: ρ for different values of p for the hierarchical tree with $(z, m) = (5, 3)$.

8 | Supplementary material - Complex Contagion

Task leader(s): *Marco Zenari*

8.1 | Generating functions derivation of cascade condition for random graphs

Suppose that we have a network with degree distribution p_k and probability that a node with degree k is vulnerable $\rho_k = P[\Phi \leq 1/k]$. Then the probability of a vertex u of having degree k and being vulnerable is $p_k\rho_k$ and correspond to the following generating function of vulnerable vertex degree:

$$G_0(x) = \sum_k p_k \rho_k x^k. \tag{8.1}$$

$G_0(x)$ generates all the moments of the degree distribution of vulnerable vertices and, as usual, the relevant moment can be extracted by evaluating the derivatives of 8.1 at $x = 1$. In particular, we can be interested in the vulnerable fraction of the population $P_v = G_0(1)$ and the average degree of vulnerable vertices $z_v = G_0'(1)$. We now consider the degree distribution of a vulnerable node v that is a random neighbor of u. v is more likely to be a neighbor of u if it has a high degree, and therefore the probability of choosing v is proportional to kp_k. The correctly normalized generating function $G_1(x)$ of a neighbor of u is given by:

$$G_1(x) = \frac{\sum_k k p_k \rho_k x^{k-1}}{\sum_k k p_k} = \frac{G_0'(x)}{z}. \tag{8.2}$$

As in traditional generating functions approaches (Ref. [14]), we consider also the analogous generating functions:

$$H_0(x) = \sum_n q_n x^n, \tag{8.3}$$

$$H_1(x) = \sum_n r_n x^n, \tag{8.4}$$

where q_n is the probability that a randomly chosen node will belong to a vulnerable cluster of size n and r_n is the corresponding probability for a neighbour of an initially chosen node. For a sufficiently large random graph, each subcluster of a finite cluster can be treated independently of the others. Therefore, the probability of a finite cluster of size n is simply the product of the probabilities of its subclusters. As shown in Ref. [14] $H_1(x)$ satisfies the self-consistency equation:

$$H_1(x) = [1 - G_1(1)] + xG_1(H_1(x)), \tag{8.5}$$

from which we can compute H_0 as

$$H_0(x) = [1 - G_0(1)] + xG_0(H_1(x)). \tag{8.6}$$

In equations 8.5, 8.6 the right hand side term consist in the probability that a given node is not vulnerable, while the left hand side consists in the size distribution of vulnerable clusters attached to a node that is vulnerable itself. H_0 generates therefore all the moments of the vulnerable cluster sizes and in particular also the average vulnerable cluster size $\overline{n} = H_0'(1)$. Note that, by definition, this is the quantity that diverges at percolation. Computing $\overline{n}$ by using equations 8.6, 8.5 and 8.2 we obtain

$$\overline{n} = G_0(1) + \frac{(G_0'(1))^2}{z - G_0''(1)}, \tag{8.7}$$

that diverges when

$$G_0''(x) = \sum_k k(k-1)\rho_k p_k = z, \tag{8.8}$$

which is the *cascade condition*.

8.2 | Heterogeneous thresholds

In the simulations described in section 4.3 we have considered only the case where the threshold is the same for all nodes. In general, the threshold can be sampled from any normalized distribution. Now we study how heterogeneous thresholds influence the cascade window. To do that we set up some simulations, again with Erdős Rényi Gilbert models, in which we sample the threshold from a Gaussian distribution. The mean of the gaussian is chosen in a similar way as in section 4.3 exploring the phase space (Φ, z), while the standard deviation has been fixed at two different values $\sigma = 0.05$ and $\sigma = 0.1$. We have implemented the simulation with 25 realizations of the network and report the empirical cascade window in Fig. 8.2, compared with the case of uniform threshold. Clearly, increasing the heterogeneity of thresholds reduces the stability of the system under random cascade failures as the cascade window is wider if the thresholds are heterogeneous.

8.3 | Barabasi Albert networks simulations and comparison with Erdős Rényi Gilbert

We have produced a similar analysis to that done in 4.3 for the Barabasi-Albert model, a growth model used to build scale-free networks. For this model, we can tune the parameter m, which is the initial degree of a node added to the network. The average degree for such a network is given by $z = 2m - \frac{m}{N} - \frac{m}{N^2}$ which tends to $z = 2m$ in the thermodynamic limit. The results and comparison with the Erdős Rényi Gilbert model are shown in Fig. 8.3. The results are compatible within the precision of the simulations (note that we only compute each realization of the parameters 25 times).

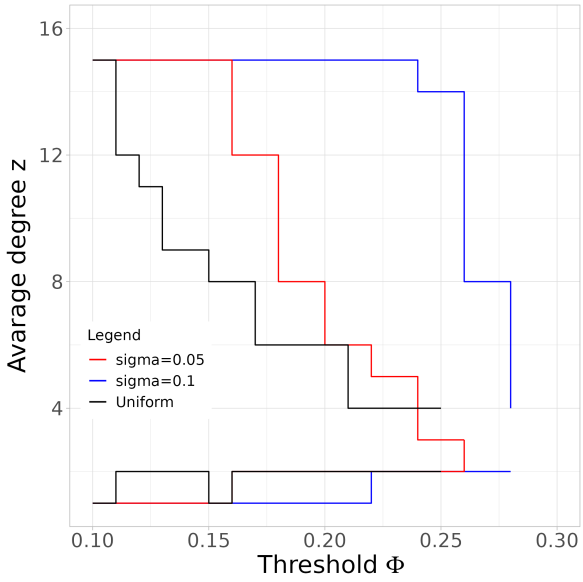


Figure 8.1: Comparison of the simulations with the same parameters for Erdős Rényi Gilbert networks evolved with threshold model using different threshold distributions: a costant threshold for each node and a normally distributed threshold with different standard deviations $\sigma = 0.05$ and $\sigma = 0.1$.

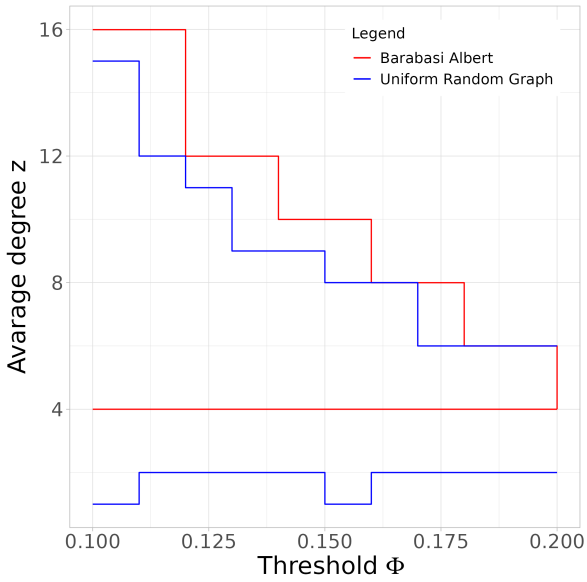


Figure 8.2: Comparison of the simulations with the same parameters for Erdős Rényi Gilbert networks and Barabasi Albert netowrks evolved with Watts threshold model.

9 | Bibliography

[1] SNAP: Network datasets: Autonomous systems - AS-733. URL http://snap.stanford.edu/data/as.html.

[2] Network data. URL http://www-personal.umich.edu/~mejn/netdata/.

[3] Preben Alstrøm. Mean-field exponents for self-organized critical phenomena. *Phys. Rev. A*, 38:4905–4906, Nov 1988. doi: 10.1103/PhysRevA.38.4905. URL https://link.aps.org/doi/10.1103/PhysRevA.38.4905.

[4] A. Arenas, A. Díaz-Guilera, and R. Guimerà. Communication in networks with hierarchical branching. *Phys. Rev. Lett.*, 86:3196–3199, Apr 2001. doi: 10.1103/PhysRevLett.86.3196. URL https://link.aps.org/doi/10.1103/PhysRevLett.86.3196.

[5] Per Bak, Chao Tang, and Kurt Wiesenfeld. Self-organized criticality: An explanation of the $1/f$ noise. *Phys. Rev. Lett.*, 59:381–384, Jul 1987. doi: 10.1103/PhysRevLett.59.381. URL https://link.aps.org/doi/10.1103/PhysRevLett.59.381.

[6] Eric Bonabeau. Sandpile dynamics on random graphs. *Journal of the Physical Society of Japan*, 64(1):327–328, 1995. doi: 10.1143/JPSJ.64.327. URL https://doi.org/10.1143/JPSJ.64.327.

[7] Charles D. Brummitt, Raissa M. D'Souza, and E. A. Leicht. Suppressing cascades of load in interdependent networks. *Proceedings of the National Academy of Sciences*, 109(12):E680–E689, 2012. doi: 10.1073/pnas.1110586109. URL https://www.pnas.org/doi/abs/10.1073/pnas.1110586109.

[8] Jean M Carlson and John Doyle. Highly optimized tolerance: A mechanism for power laws in designed systems. *Physical Review E*, 60(2):1412, 1999.

[9] P. Echenique, J. Gómez-Gardeñes, and Y. Moreno. Dynamics of jamming transitions in complex networks. *Europhysics Letters*, 71(2):325, jun 2005. doi: 10.1209/epl/i2005-10080-8. URL https://dx.doi.org/10.1209/epl/i2005-10080-8.

[10] Pablo Echenique, Jesús Gómez-Gardeñes, and Yamir Moreno. Improved routing strategies for internet traffic delivery. *Phys. Rev. E*, 70:056105, Nov 2004. doi: 10.1103/PhysRevE.70.056105. URL https://link.aps.org/doi/10.1103/PhysRevE.70.056105.

[11] K.-I. Goh, B. Kahng, and D. Kim. Universal behavior of load distribution in scale-free networks. *Phys. Rev. Lett.*, 87:278701, Dec 2001. doi: 10.1103/PhysRevLett.87.278701. URL https://link.aps.org/doi/10.1103/PhysRevLett.87.278701.

[12] K.-I. Goh, D.-S. Lee, B. Kahng, and D. Kim. Sandpile on scale-free networks. *Phys. Rev. Lett.*, 91:148701, Oct 2003. doi: 10.1103/PhysRevLett.91.148701. URL https://link.aps.org/doi/10.1103/PhysRevLett.91.148701.

[13] Adilson E. Motter and Ying-Cheng Lai. Cascade-based attacks on complex networks. *Phys. Rev. E*, 66:065102, Dec 2002. doi: 10.1103/PhysRevE.66.065102. URL https://link.aps.org/doi/10.1103/PhysRevE.66.065102.

[14] Mark EJ Newman, Steven H Strogatz, and Duncan J Watts. Random graphs with arbitrary degree distributions and their applications. *Physical review E*, 64 (2):026118, 2001.

[15] Thomas C Schelling. Hockey helmets, concealed weapons, and daylight saving: A study of binary choices with externalities. *Journal of Conflict resolution*, 17(3): 381–428, 1973.

[16] Duncan J Watts. A simple model of global cascades on random networks. *Proceedings of the National Academy of Sciences*, 99(9):5766–5771, 2002.