6 Cascading Reactions on Networks

6.1 Introduction

The phenomena of *cascading reactions* and, in particular, *cascading failures* are quite similar to virus spreading over various complex networks. In many real-world networks, intentional attacks or unexpected failures on a few nodes may cause severe chain reactions through the connections among nodes, leading to collapse of a large portion of the network or even the entire network. This is also called *avalanche*. One example in point is the Internet, where attacks on a few routers can cause overloading of some nearby routers which consequently redistribute their loads to other routers; this eventually lead to data-traffic congestion of some parts of the network. In electric power grids, as another example, failures of some local facilities or devices such as generators and transmission lines can lead to blackout of a large area of residence and industry. The well-known Northeast Blackout in 2003 was a massive power outage that occurred throughout a large region of the northeastern United States and Ontario Canada on Thursday 14 August 2003, the largest blackout in North America's history, which reportedly affected about 10 million people in the province of Ontario (about 1/3 of the population of Canada) and 40 million people in eight U.S. states (about 1/7 of the population of USA) and caused financial losses of about $6 billion USD. To prevent such disasters from happening, understanding how cascading failures are propagating over complex networks is extremely important and also very urgent. This chapter is devoted to a study of the cascading reactions over complex networks.

6.1 Dynamic Cascading Failures: Models and Analyses

6.2.1 Models Based on Node Dynamics

Fiber-Bundle Model

The so-called Fiber-Bundle Model (FBM) is a conceptual graph framework for cascading failure analysis on networks [1]. In the FBM, a set of large N fibers (nodes) are located on the sites of a lattice, and each element is randomly assigned a security threshold, σ_i , $i = 1,2,...,N$, sampled from a given probability distribution—typically the Weibull distribution. Then, the nodes are loaded against the values, σ_i , $i = 1,2,...,N$. If a node i is loaded by σ , which is higher than its threshold value σ_i , then this node is considered failed, $i = 1,2,...,N$. The individual load carried by each of the failed nodes is then equally transferred through connecting edges to their surviving nearest neighbors; therefore, the rupture of a node may induce secondary failures which, in turn, may trigger tertiary failures, and so on.

These kinds of networks are usually designed conservatively, in such a way that when all loads at nodes are being balanced to below their respective security thresholds, a global equilibrium will be attained and then retained, unless new failures happen again.

As mentioned above, the security thresholds of nodes follow the Weibull distribution. The Weibull cumulative distribution function is

$$P(\sigma_i) = 1 - e^{-(\sigma_i)^{\rho}} \tag{6-1}$$

where ρ is the Weibull exponent, which controls the degree of threshold disorder in the network—the bigger the value of ρ, the narrower the range of the threshold values. This allows one to compare the stability of different networks with different levels of heterogeneity in their security threshold distribution.

Figure 6-1 [1] shows the largest connected sub-network versus the network load σ when a cascading failure process is ended at equilibrium on a BA scale-free network of size $N = 10^5$. In this figure, the vertical axis is the fraction of largest connected sub-net in the whole network, and the three curves correspond to one random-graph network and two different FBM networks with $\rho = 5$ and $\rho = 2$ in their Weibull threshold distributions (6-1), respectively.

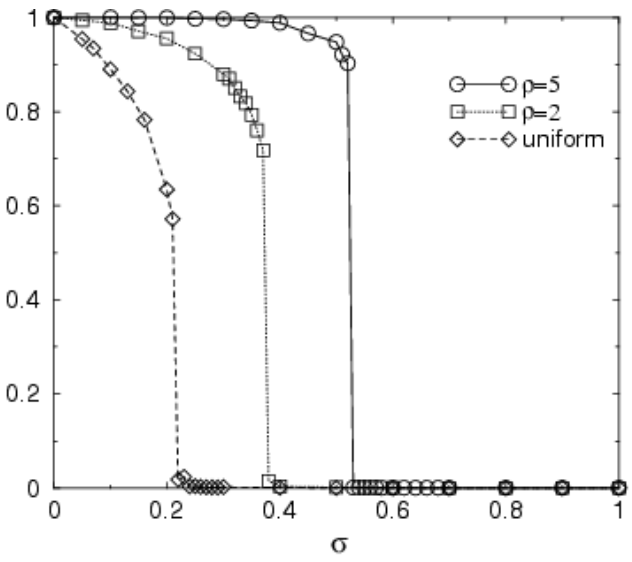


Fig. 6-1 Fraction of remaining largest connected sub-nets versus security threshold [1]

It can be seen from Fig. 6-1 that for smaller σ, i.e., with lower loading at nodes, the remaining fraction of connected sub-nets is larger, i.e., the failure damage on the whole network is less severe. It is also clear that when the network load σ is increased to a certain critical value, σ_c, the curves suddenly fall down to zero, implying that the whole network has fell in many small pieces therefore completely

collapses. Here, it should be noted that increasing the ρ value will move the σ_c value to the right, which means that if the security thresholds σ_i, $i = 1,2,...,N$, are distributed more evenly, the network is more robust against overloading.

The parameter σ can be used to control the network topological features. Figure 6-2 [1] shows the distribution P_k of degree-k nodes versus k, for some different σ values. It can be seen from the figure that when the network load is relatively small (e.g., $\sigma = 0.05$), the network topology remains unchanged, but when the network load is larger than a threshold $\sigma_c = 0.52$ the network is about to collapse; therefore, there are no big nodes in the remaining part of the network.

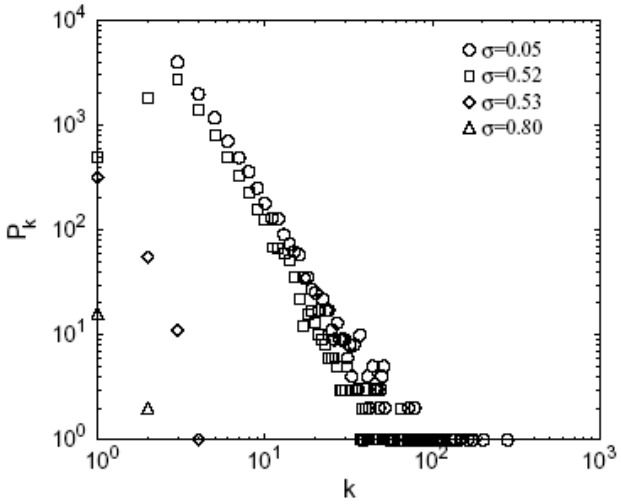


Fig. 6-2 For different σ, the distribution P_k of degree-k nodes versus k [1]

Betweenness-Based Model

Another cascading failure model is based on the concept of betweeness [2]. For a network of size N, assume that data (or information, energy, etc.) are transmitted through the shortest paths between nodes and that the load at a node is measured by the node betweenness (Section 4.2.5, Chapter 4).

Let the maximum-load capacity of node i be proportional to its initial loading L_i:

$$C_i = (1+\alpha)L_i, \qquad i = 1,2,...,N, \tag{6-2}$$

where constant $\alpha \geq 0$ is the tolerance parameter. In a normal situation, there are free flows traversing on the network. When a node fails to work, traffic cannot go through it, so in this case the node is considered being separated from the largest connected sub-net. Consequently, the traffic data have to be redistributed over the rest of the network, which generally change the loads of the remaining nodes and the distribution of the shortest paths. Clearly, for heterogeneous networks, the failure of big nodes can easily cause network traffic congestion eventually to collapse.

Similar to Fig. 6-1, the fraction G of remaining connected sub-net over the whole network is used as a measure of the network performance. The AS-level Internet data [3] show that if the node failure occurs randomly, then the network connectivity of G is almost unchanged; yet if some big nodes fail then G will decrease

significantly, even when α increases to 1. Even nodes take loads as high as twice of the initial loads, G will still decrease for about 20%, as shown in Fig. 6-3 [2].

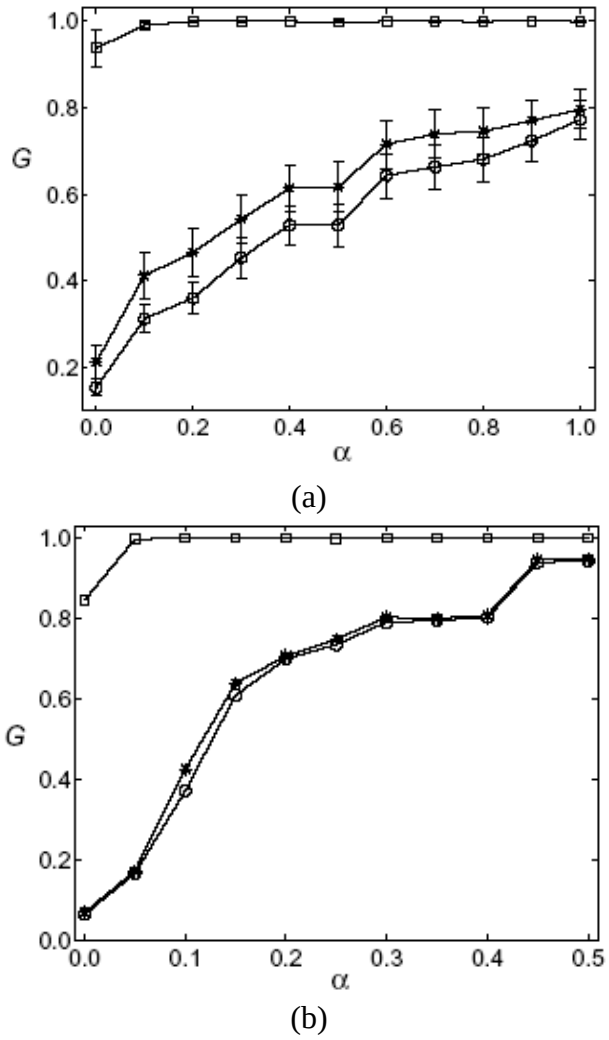


Fig. 6-3 Performance on cascading failures [2]:
(a) Scale-free network (b) AS-level Internet

In Fig. 6-3 [2], square curves correspond to random node failures, star curves to largest-degree node failures, and circle curves to biggest-betweenness node failures. It is clear that for the scale-free network, in the case of largest-degree node failure, the smaller the α, the worse the performance.

Figure 6-4 [3] compares the performance of a random-graph network and a scale-fee network, both have $N = 5{,}000$ and about the same average degree $\langle k \rangle \approx 3$. For small $\alpha = 0.05$, the random-graph network remains intact against both random as well as intentional attacks. In comparison, the scale-free network is damaged up to 90% under the same two attacks. This clearly shows that homogeneous networks are much more robust than heterogeneous ones against cascading failures.

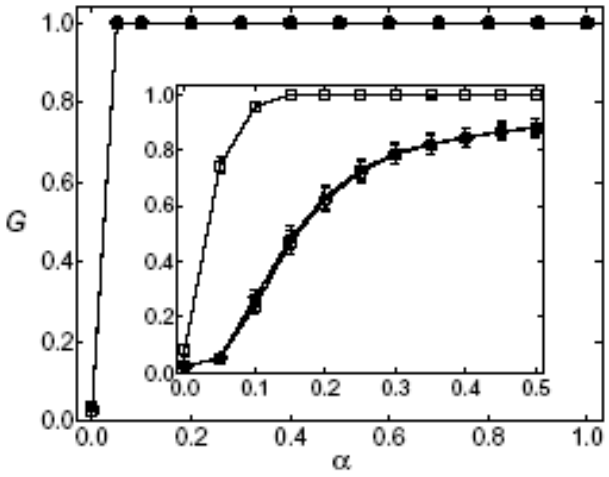


Fig. 6-4 Comparison of cascading failures on random and scale-free networks [3]

Next, consider a network on which the load of a node is measured by its node betweenness, but the maximum-load capacity of the node is defined by two different measures: (i) the maximum-load capacity increases linearly as the number of nodes increases; (ii) the maximum-load capacity is constant. Regarding the network, if it grows according to the BA power law, then when nodes and edges increase to a certain number, respectively, some nodes will be overloaded because the node-betweenness will be higher than its maximum-load capacity. Thus, these nodes and their connecting edges will be removed, and consequently the betweenness of the remaining nodes will have to be recalculated. Repeat this process until no overloaded nodes remaining on the network.

Simulations show that in case (ii) cascading failures are basically unavoidable, because the capacity of each node is fixed. Also, comparing a scale-free network with the BA preferential attachment scheme to a scale-free network with a random attachment scheme, the former is faster to encounter cascading failures.

Figure 6-5 [4] shows the changes of the largest connected sub-net G, number of edges M and reciprocal of average path length L^{-1}, versus time t, in a scale-free network with the BA preferential attachment scheme. Their maximum values are $G_{\max}=159$, $M_{\max}=1133$, $L^{-1}_{\max}=0.2914$, respectively. Figure 6-6 [4] shows the corresponding changes in a scale-free network with a random attachment scheme, where $G_{\max}=207$, $M_{\max}=2030$, $L^{-1}_{\max}=0.2929$, respectively. The two figures have been normalized, so that these curves can be drawn in the same figure for visualization. It can be seen from the two figures that all three curves first move up and then move down, implying that when the networks grow to certain sizes some nodes start to fail due to overloading, leading to disconnection of the networks. Even for a network with capacity measure (i), although the node capacities are in the same order of the node number N, their loadings are in the order of N^{α}, where $\alpha>1$, so the network will still collapse as N becomes large enough.

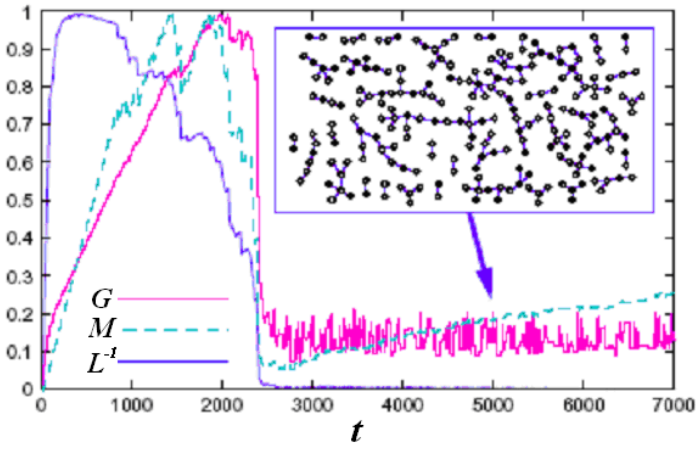


Fig. 6-5 Changes of parameters G, M, L^{-1}: First case [4]

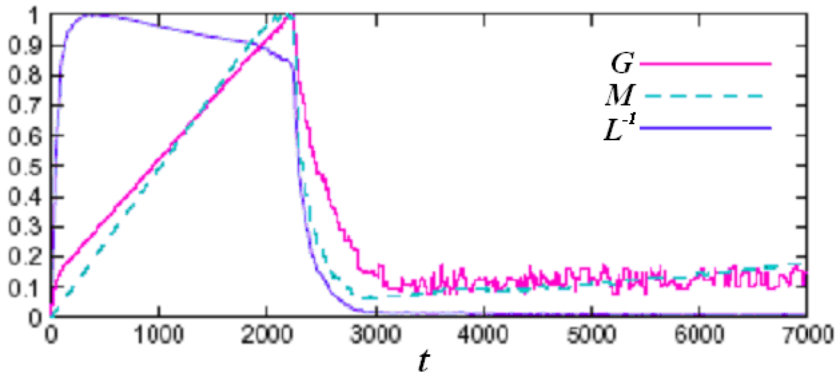


Fig. 6-6 Changes of parameters G, M, L^{-1}: Second case [4]

6.2.2 Models Based on Edge Dynamics

Since the edge dynamics can also affect the cascading failure processes, actually often quite significantly, edge characteristics should also be taken into account in network failure modeling.

Let the edge loading be denoted by $\ell_{i,j}$, normally $0 < \ell_{i,j} < 1$, which represents the flow volume (capacity, bandwidth, etc.) of the edge between node i and node j, satisfying the following distribution:

$$U(\ell) = \begin{cases} \dfrac{1}{2\langle \ell \rangle} & \ell \in [0, 2\langle \ell \rangle], \quad \langle \ell \rangle \le 0.5 \\ \dfrac{1}{2(1-\langle \ell \rangle)} & \ell \in [2\langle \ell \rangle - 1, 1], \quad \langle \ell \rangle \ge 0.5 \end{cases} \tag{6-3}$$

where $\langle \ell \rangle$ is the average loading over the whole network. Suppose that the maximum-load capacity of each edge is $C = 1$. Thus, if $\ell_{i,j} > C$, then this edge encounters congestion. Consequently, the total edge loads will be redistributed according to a certain rule, for instance evenly redistributing all the loads to all neighboring edges or redistributing part of the loads from the congested edge to some other un-congested neighboring edges; if all its neighboring edges are also congested, then redistributing the loads to all other edges globally, or simply dropping the data

packets. Obviously, the redistribution of data flows may lead to new congestions on other edges, thus causing cascading failures elsewhere. If there are too many congested edges, the network may become unconnected in terms of data traffic.

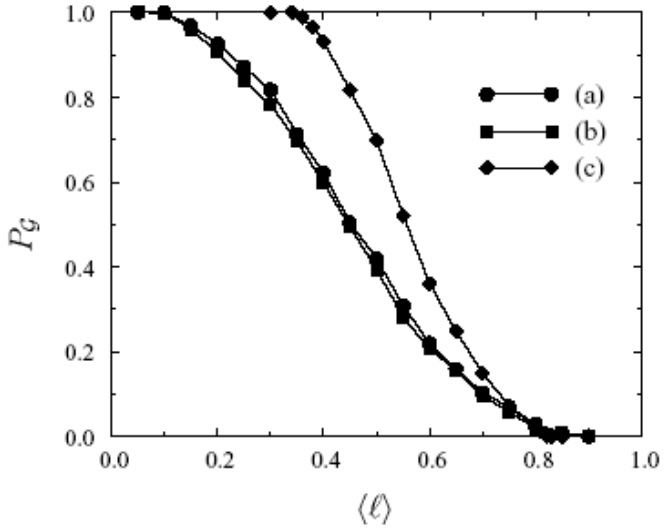


Fig. 6-7 Relation between P_g and $\langle \ell \rangle$ [5]

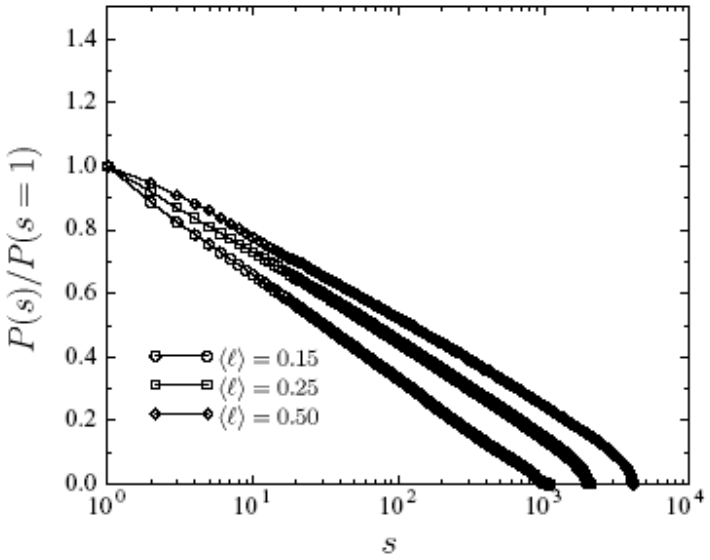


Fig. 6-8 Cumulative probability distribution of s under different $\langle \ell \rangle$ [5]

Simulations on BA scale-free networks show that when a network is stable, namely, $\ell_{i,j} < C$ for all $i, j = 1,2,...,N$, there is a threshold $\langle \ell \rangle_c^{\ I}$ of load redistribution: if $\langle \ell \rangle > \langle \ell \rangle_c^{\ I}$, then with a certain probability the network will be congested; while if $\langle \ell \rangle > \langle \ell \rangle_c^{\ II} \approx 0.82$ (from the simulations), then any instability will lead to global congestion over the entire network. Figure 6-7 [5] shows the relation between the probability P_g of retaining a largest connected sub-net and the average loading $\langle \ell \rangle$, on a BA scale-free network with 10^4 nodes and 3×10^4 edges, where the three curves are: (a) randomly redistributing (or dropping) the loads from the congested

edges, (b) randomly or globally redistributing the loads from the congested edges, and (c) uniformly or globally redistributing the loads from the congested edges. It can be seen that for medium-sized $\langle \ell \rangle$, the number s of simultaneously overloading edges approximately follows a power-law distribution with $\gamma \approx 1$. Figure 6-8 [5] shows the cumulative probability distribution of s under different average loadings.

The concepts of loading and capacity may be defined in some different ways [6]. During the growth of a BA scale-free network, a new node brings in m new edges to connect to existing nodes. For a small m, if the network grows according to the BA preferential attachment scheme, then when the network size is increasing to a certain level the largest connected sub-net will attain its maximum. Then, some edges will be overloaded, therefore the traffic data will be redistributed or dropped, so that the network will gradually reach an equilibrium state. In this case, the network as a whole will not be connected, due to the removal of the above congested edges, but there usually will be a cluster of nodes that is bigger than the others, as shown in Fig. 6-9 [6]. In the figure, dash curves represent the networks with the preferential attachment (PA) scheme and solid curves, the networks with the random attachment (RA) scheme. It can be seen from Fig. 6-9 (a) that in the random attachment case, overloading occurs later and its equilibrium s size is larger than the preferential attachment case. This means that overloading does not affect the network topology very significantly. It can also be seen from Fig. 6-9 (b) that the decreasing of the M curves is not as prominent as the s curves, implying that overloading of a few edges can lead to significant decrease of s. This is because the few edges between the connected sub-nets have very large amounts of traffic, thereby becoming congested first when the network grows to be large. Figure 6-9 (c) shows the changes of the average path lengths L, which decreases to its minimum in the earlier stage of the network growth, and then continuously increases as the network becomes bigger and bigger, consequently yielding more and more disconnected parts.

Comparing the overloading of nodes and the overloading of edges, one can see that in the former case there will be mutually disconnected clusters after cascading failures have occurred, while in the latter case there will be large cluster(s) left out in the network. Moreover, scale-free networks with the random attachment scheme are more robust against traffic congestion due to node or edge overloading.

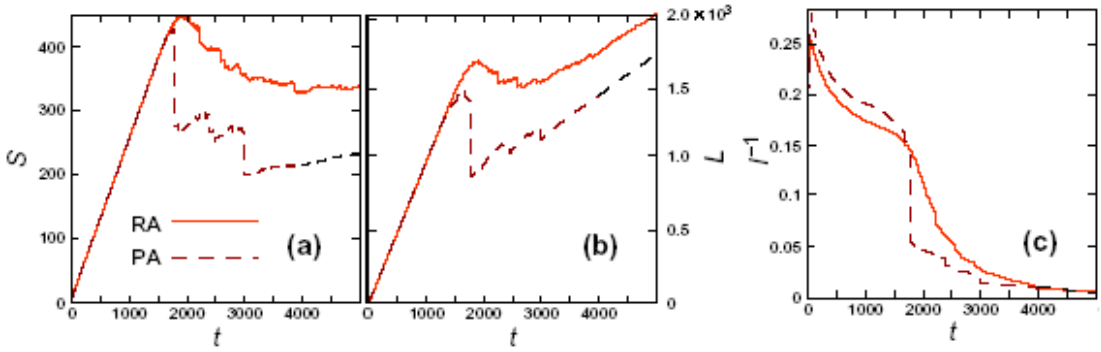


Fig. 6-9 The s, M, L^{-1} curves in scale-free networks with RA or PA schemes [6]

6.2.3 Hybrid Models Based on Node and Edge Dynamics

It is possible to take into account both node and edge dynamics in a cascading failure model.

For example, one model [7] uses an undirected weighted network G to model a communication or transportation system, in which the weight on the edge between node i and node j is denoted by $e_{ij} \in [0,1]$: the bigger the e_{ij}, the more efficient the data traffic. Thus, the $N \times N$ coupling matrix $\{e_{ij}\}$ describes the efficiency of communications among nodes. Initially, set all $e_{ij} = 1$. Let $L_i(t)$ be the loading of node i at time t, representing the number of efficiency-optimal paths that pass through node i. Here, for all paths that pass through the edge between the node pair (i, j), the *efficiency-optimal path* is the one that maximizes $e^* = \sum (1/e_k)^{-1}$, and is denoted by $e^*_{\max}$. The capacity of node i is defined to be $C_i = \alpha \cdot L_i(0)$, where constant $\alpha \geq 1$ is a tolerance parameter. Also, define the evolution of weights by

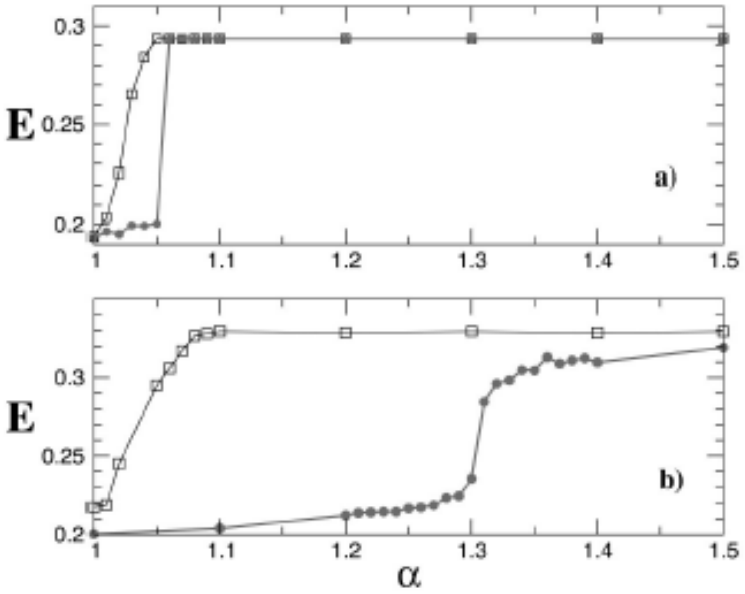
$$e_{ij}(t+1) = \begin{cases} e_{ij}(0) \cdot \dfrac{C_i}{L_i(t)} & , L_i(t) > C_i \\ e_{ij}(0) & , L_i(t) \leq C_i \end{cases} \tag{6-4}$$

After a node failed and so being removed, all the relevant efficiency-optimal paths will be changed, leading to a redistribution of loads which may cause overloading to some nodes. This, in turn, may lead to another round of load-redistribution, eventually leading to cascading failures.

To measure the level of destruction, define the average efficiency of the network by

$$E(\mathrm{G}) = \frac{1}{N(N-1)} \sum_{i \neq j} e_{ij} \tag{6-5}$$

When this model is applied to an ER random-graph network and a BA scale-free network of the same size with $N = 2{,}000$ and $M = 10{,}000$, a comparison is given in Fig. 6-10 [7], in which the empty squares are the results of randomly removing nodes and the solid circles are the results of intentionally removing biggest nodes. It can be seen that both networks have their threshold values α_c: when $\alpha < \alpha_c$, the network collapses, with $E(G) < 0.25$. But the threshold of the ER network is much smaller than that of the BA network, showing that ER random-graph networks are more robust than the BA networks in resisting cascading failures. Besides, for both ER and BA networks, the node-removal scheme based on loadings is easier to create cascading failures than the random removal scheme. This is consistent with the results observed from Fig. 6-4 above.



(a) the ER network; (b) the BA network

Fig. 6-10 Average efficiency E versus tolerance parameter α [7]

A power grid can be viewed as a network with nodes being power generators and edges being power lines. It has been observed that the North America's power grid, for example, approximately follows a power-law node distribution [8], with a semi-log plot shown in Fig. 6-11 [8], where K is the node degree. Furthermore, if the betweenness is used as the loading measure, then the North America's power grid has a precise power-law distribution in terms of load distribution, as shown in Fig. 6-12 [8], where L is the average path length of the grid.

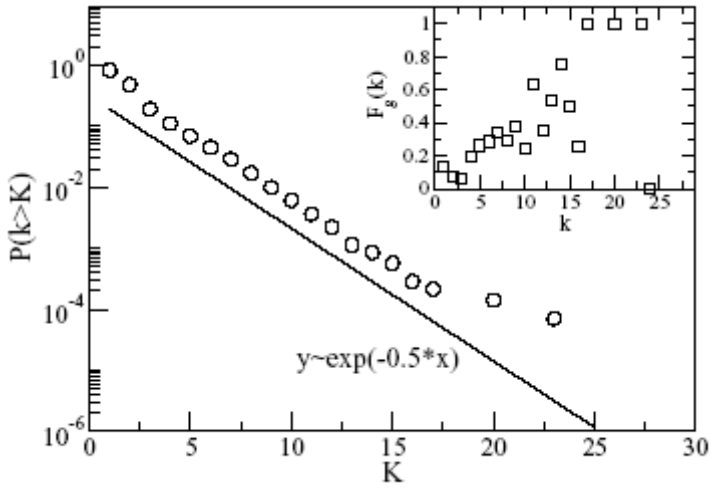


Fig. 6-11 Probability distribution of nodes with degrees larger than K [8]

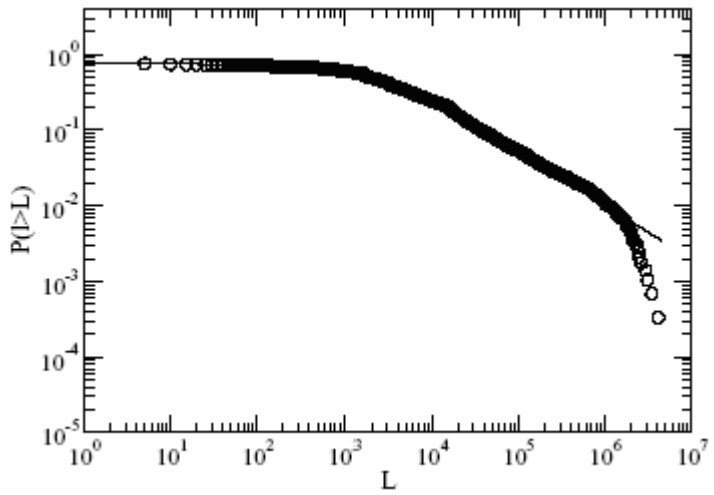


Fig. 6-12 Probability distribution of average path lengths being larger than L [8]

When the above model is applied to the North America's power grid data [7], where the failed nodes (generators or transmission plants) with biggest loads are being removed, the other nodes would become overloaded, so that the steady-state value of the network average efficiency in terms of $E(G)$ becomes lower than the normal situation with $E(G_0) = 0.04133$. Moreover, as α decreases, this decrease of $E(G)$ becomes more severe; on the contrary, random failed-node removal does not have prominent effects. Figure 6-13 shows a comparison of these two removal schemes, where triangles correspond to random removal while circles to load-based removal, with minimal value $E(G_0) = 0.04133$ when no overloading occurs. It is clear that as the tolerance value α increases, the steady-state values of $E(G)$ approach the initial values, meaning that if tolerance is relaxed then overloading will become less serious, consistent with the common intuition.

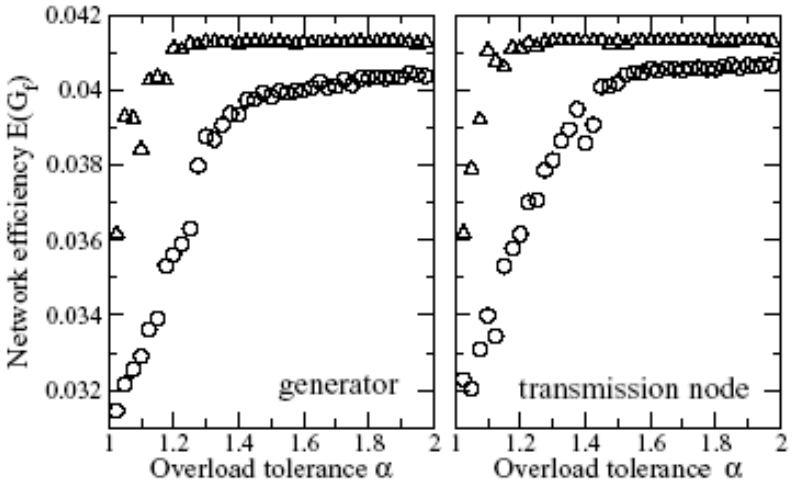


Fig. 6-13 Efficiency $E(G)$ versus tolerance α [9]

Further analysis reveals that node removal due to failures may be classified into three types according to their effects on the network efficiency: (i) nodes with small degrees and loads, which do not significantly affect the network efficiency after being removed, constitute about 60% of the total; (ii) nodes with large degrees or loads,

which will significantly affect the network efficiency after being removed, constitute about 20% of the total and are typically dependent on the tolerance parameter α; (iii) nodes have effects on network efficiency when α is small but the effects are fading out as α becomes large.

Define the efficiency loss by

$$D = (E(G_0) - E(G_f))/E(G_0) \tag{6-6}$$

where $E(G_f)$ is the steady-state efficiency and $E(G_0)$ is the initial efficiency of the network. Figure 6-14 shows the distributions of the efficiency loss D versus the tolerance α, where the distribution of D approximately follows a power-law form with $\gamma = 1.1$, consistent with some other reports [10,11]. This implies that if one big node is removed at a time, then the first removal has the biggest effect on the efficiency of the network.

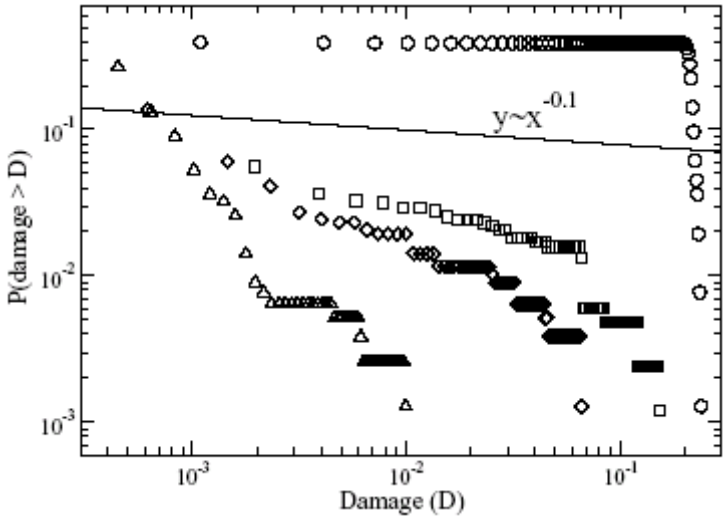


Fig. 6-14 Cumulative distributions of network efficiency loss D [9]: α =1.025 (circles); α =1.2 (squares); α =1.4 (diamonds); α =1.8 (triangles)

6.2.4 Binary Influence Model

The so-called binary influence model is a special case of a general influence model [12], which can be applied to analyzing the mechanisms and effects of cascading failures [13].

Construct a random-graph network model with N nodes, node distribution $P(k) = p_k$, and average degree $\langle k \rangle = z$. Assume that each node has only two states, 0 (normal state) and 1 (failure), and at any time a node determines its state according to the states of its k neighbors. Let $N_1(k)$ be the number of nodes with value 1 in the k neighbors of a node, which clearly has degree k, and ϕ be the threshold of state change of this node, with density $F(\phi) = \delta(\phi - \phi_*)$, a delta distribution centered at a

constant value ϕ_*.

Initially, at $t = 0$, most nodes have value 0 but a small fraction of nodes have value 1. After started, the state of a node is determined by the following rules: If $N_1(k)/k \geq \phi$ then the state of this node is 1; otherwise, 0. If the state of a node becomes 1 at some time, then it will stay to be 1 forever thereafter, meaning that no repairing of failed nodes is performed.

It turns out that when the degree distribution p_k and threshold ϕ satisfy a certain relation, avalanche may occur.

Define the generating function of susceptible nodes (with at least one neighbor having a threshold value $\phi \leq 1/k$) by

$$G_0(x) = \sum_k \rho_k p_k x^k \tag{6-7}$$

where

$$\rho_k = \begin{cases} 1 & k = 0 \\ F(1/k) & k > 0 \end{cases} \tag{6-8}$$

When $G_0^{"}(1) < z$, there are very few susceptible nodes in the network, therefore no significant cascading failures would happen. Conversely, random failures of individual nodes could cause severe cascading failures.

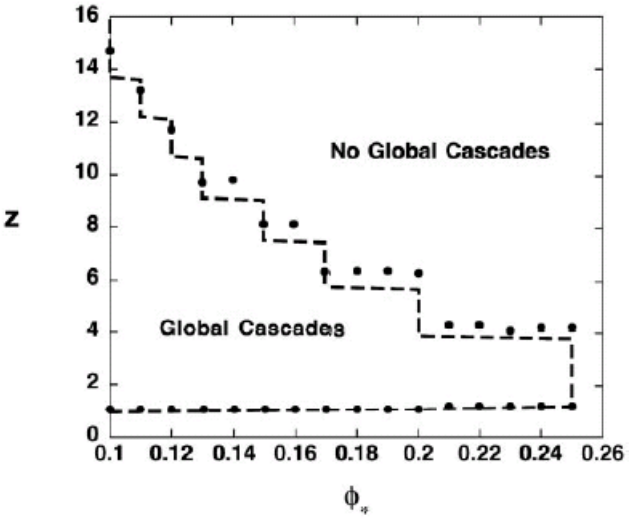


Fig. 6-15 Boundary of cascading failures [12]

Figure 6-15 [12] shows the critical boundary of global cascading failures on networks with homogeneous degree and threshold distributions, where solid dots are simulated results and the dashed curve is the theoretical result. It shows that within the region of the curves, any combination of degree and threshold distributions will cause

cascading failures, but outside which any combinations will not. It implies that if the internal connections of a network are not too dense then the propagation of cascading failures is determined by the global connectivity; otherwise, by the local stability of individual nodes.

The heterogeneity of network connectivity has mixed effects on the network stability. On one hand, increasing the heterogeneity of the individual node-failing thresholds can easily cause global failures; on the other hand, increasing the heterogeneity of the node-degree distribution can decrease the possibility of global failures. Figure 6-16 [12] compares the failure boundaries: (a) for different heterogeneities of node-failing thresholds, where σ is the standard deviation of threshold samples (the bigger the σ, the higher the heterogeneity); (b) for homogeneous and heterogeneous networks, where the latter has a smaller region of cascading failures.

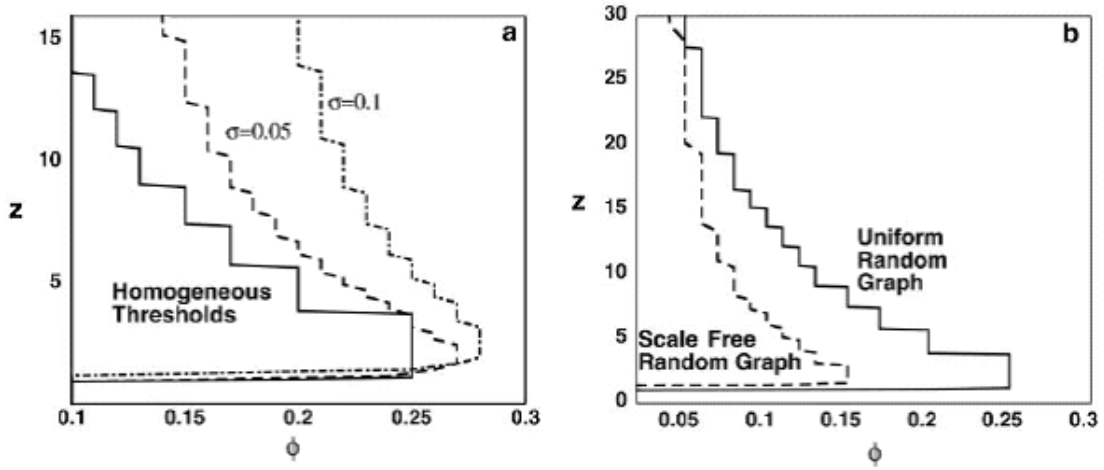


Fig. 6-16 Comparisons of boundaries of cascading failures [12]

6.2.5 Sand-Pile Model

The now-well-known sand-pile model was proposed by three physicists, Bak, Tang and Wiesenfeld, at the US Brookhaven National Lab in 1987 [14]. This is the first example of a dynamical system displaying self-organized criticality. The model is by nature a cellular automaton. At each site on the lattice there is a value that corresponds to the slope of the pile. This slope builds up as grains of sand are randomly placed onto the pile, until the slope exceeds a specific threshold value and, at that moment, this site collapses thereby transferring the sand into its adjacent sites, which increases their slopes. This random placement of sand may have no effect on an individual site but it may cause cascading reactions that can affect every site on the lattice, finally leading to avalanche.

More precisely, the sand-pile model is constructed as follows [14]:

1) Every node i has a "height" (load), represented by an integer h_i, and a threshold z_i satisfying $\lceil z_i \rceil \le k_i$, where $\lceil z_i \rceil$ is the smallest integer larger than z_i;

2) Randomly select a node i, and let $h_i \leftarrow h_i + 1$;

3) If $h_i > z_i$, which means node i is in an unstable state, perform a "toppling" operation: randomly select $\lceil z_i \rceil$ nodes from its k_i neighbors, and for each chosen neighboring node j, let $h_j \leftarrow h_j + 1$; meanwhile, let $h_i \leftarrow h_i - \lceil z_i \rceil$;

4) If in step 3) there was any unstable new node then perform the toppling operation in parallel, until no unstable new node will be generated.

Repeat the above steps 2) - 4) to generate a distribution of cascading failures.

A study of sand-pile model dynamics on ER networks shows that the distribution of avalanches follows a power-law distribution, with $\gamma = 1.5$ [15] or $\gamma = 1.65$ under a slightly different model [16,17]. If the threshold of node i is assumed to be $z_i = k_i^{1-\eta}$, $0 \le \eta < 1$, then on BA networks both the size s and time t of avalanches follow power-law distributions:

$$p(s) = \begin{cases} s^{-(\gamma-2\eta)/(\gamma-1-\eta)} & (2 < \gamma < 3-\eta) \\ s^{-3/2}(\ln s)^{-1/2} & (\gamma = 3-\eta) \\ s^{-3/2} & (\gamma > 3-\eta) \end{cases} \tag{6-9}$$

$$\ell(t) = \begin{cases} t^{-(\gamma-1-\eta)/(\gamma-2)} & (2 < \gamma < 3-\eta) \\ t^{-2}(\ln t)^{-1} & (\gamma = 3-\eta) \\ t^{-2} & (\gamma > 3-\eta) \end{cases} \tag{6-10}$$

which generalizes the results reported in [19] where $z_i = k_i$, i.e., $\eta = 0$.

It can be seen from (6-9) and (6-10) that for $2 < \gamma < 3-\eta$, the exponents τ and δ decrease as γ increases. For a network with fixed size, the smaller the γ, the larger the node degree, and the higher the τ and δ. This implies that the influence of the failures reduces, therefore the hub nodes in a BA network take the major part of the loading, which enhances the robustness of the network against cascading failures. Note that this observation is not conflicting with the conclusion of [2], discussed above in Fig. 6-3, since in the sand-pile model the selection of nodes is a random process, and random failures do not have significant influence on scale-free networks.

When $\gamma > 3-\eta$, both exponents τ and δ are constants, being 1.5 and 2, respectively, implying that the size and time of cascading failures do not rely on the detailed network connectivity.

Moreover, if the thresholds z_i only take two values: z_i = 1 if $k_i = 1$, and z_i = 2, otherwise, then $\tau = 1.5$ and $\delta = 2$ ($\gamma > 2$). In this case, even noise does not affect very much the distributions of size and time of the cascading failures [18].

6.2.6 OPA Model

The so-called OPA model is the ORNL-PSerc-Alaska model used to study the blackout dynamics in power transmission grids, where ORNL stands for Oak Ridge National Laboratory and PSerc for Power Systems Engineering Research Center, both in the USA. The model represents transmission lines, loads and generators with the usual DC load flow assumptions. Blackouts are initiated by a random line outage. When a line is outaged, the generation and loads are re-dispatched using standard linear programming. If any lines were overloaded during the optimization then these limes are outaged with a certain probability. The process of re-dispatch and testing for outages is iterated until there are no outages. Thus, the OPA model can represent generic cascading outages (failures), which are consistent with network and operational constraints [20-24].

The OPA model involves two intrinsic time scales. There is a slow time scale, in the orders of days to years, over which load-power demand slowly increases and the network is upgraded in engineering responses to blackouts. Both of the slow process opposing load increase and slow network upgrade will self-organize the system to a dynamic equilibrium. On the other hand, there is a fast time scale, in the order of hours or even minutes, over which cascading failures occur and propagate fairly quickly.

Slow Time Scale

Suppose that the network has N nodes, which are separated into two groups, loads and generators, and assume that generators have no failures. Define the load power be negative and the generator power be positive, with DC loads, in the undirected network model. Let P_{ik} be the power at node i on day k, P_k be the vector of all such powers of the whole grid on day k, i.e., $P_k = (P_{1k}, P_{2k}, P_{3k}, \cdots, P_{Nk})^T$. All powers should be balanced: $\Sigma_i P_{ik} = 0$. Denote by M the number of transmission lines and let F_{jk} be the power flows of line j on day k, with the vector $F_k = (F_{1k}, F_{2k}, F_{3k}, \cdots, F_{Mk})^T$ similarly defined, which is limited by its maximum capacity:

$$-F_{jk}^{\max} \le F_{jk} \le F_{jk}^{\max}, \qquad j = 1, 2, \cdots, M$$

In the OPA model, all power lines are considered as ideal inductors without power loss in transmissions. Thus,

$$F_k = AP_k$$

where A is a constant.

Let λ_ℓ be the ratio of loads on day ℓ and on day $\ell-1$. Then,

$$P_k = P_0 \prod_{\ell=1}^{k} \lambda_\ell$$

where $\lambda_1, \lambda_2, \lambda_3, \cdots$ are independent and identically distributed with mean value slightly larger than 1. Similarly,

$$F_k = AP_k = AP_0 \prod_{\ell=1}^{k} \lambda_\ell = F_0 \prod_{\ell=1}^{k} \lambda_\ell$$

When a transmission line fails, its load capacity $F_{jk}^{\max}$ will generally be enlarged, so as to avoid the failure to repeat; namely, if failure occurs at line j on day k, then

$$F_{j(k+1)}^{\max} = \mu_k F_{jk}^{\max}$$

where μ_1, μ_2, $\mu_3, \cdots$ are independent and identically distributed parameters, satisfying $1 < \lambda_{\max} < \mu_{\min}$.

Furthermore, as loading increases, the capacities of the generators should also increase, namely,

$$P_{ik}^{\max} = (\overline{\lambda})^{k+1} P_{i0}^{\max}$$

Finally, define the fraction of overloading for a given transmission line as

$$M_{jk} = \frac{F_{jk}}{F_{jk}^{\max}}$$

Thus, all M_{jk} will approach 1 gradually.

Fast Time Scale

Suppose that the power grid encounters a failure on day k. Let f_j be the power load of line j at the moment of failure, and vector f be the load power of the line: $f = (f_1, f_2, f_3, \cdots f_m)^T$. Moreover, let p_i be the power of node i at the moment of failure, with vector p be the power of all nodes: $p = (p_1, p_2, p_3, \cdots p_n)^T$. Initialize the situation by

$$f = F_k \tag{6-11}$$

$$p = P_k \tag{6-12}$$

Typically, a power line has two types of failures: one is random failure without overloading, caused by such as weather and human errors, with a small probability denoted by

$$P\{\text{line } j \text{ outaged}\} = h^0(M_{jk}) \tag{6-13}$$

where h^0 is a positive non-decreasing function; another is overloading failure, with

a high probability denoted by

$$P\{\text{line } \ j \ \text{ outaged}\} = h^1(M_{jk}) \tag{6-14}$$

where h^1 is a positive non-decreasing function, satisfying $h^1 >> h^0$.

Power Distribution Control

When there is power line failure, overloading, or over-limit of a power generator, the total power must be redistributed over the whole grid to reach a new balance. This adjustment is usually done via linear programming, with a cost function defined by

$$\sum_{generators} | p_i - P_{ik} | + \sum_{loads} 100(p_i - P_{ik}) \tag{6-15}$$

in which the coefficient of power generation is 1 while that of power loading is 100, in order to reduce the power usage restriction while satisfying the power generation requirement. The following four constraints are imposed:

$$\sum_{i=1}^{n} (p_i - P_{ik}) = 0 \tag{6-16a}$$

$$-F_{jk}^{\max} \le f_j \le F_{jk}^{\max}; \qquad j = 1,2,\cdots,m \tag{6-16b}$$

$$P_{ik} \le p_i \le 0 \tag{6-16c}$$

$$0 \le p_i \le P_{ik}^{\max} \tag{6-16d}$$

Failure Propagation Scheme

1) initialize the scheme according to (6-11) – (6-12);

2) determine the power line failure according to (6-13);

3) perform the linear programming (6-15)–(6-16) to redistribute the network powers;

4) determine if there is overloading failure according to (6-14): if $P\{\text{line } \ j$ outaged$\} = 0$, then stop; otherwise, if P {line j outaged} = 1, return to step 2).

Various Issues on Power-Grid Failures

In the OPA model, the parameter μ is a main control parameter, which directly affects the statistical properties of the size and time (frequency) of the power blackout, as shown by Figs. 6-17 and 6-18 [21]. These simulations show that at the start, as μ increases both the size and frequency of the blackout will decrease; while as the process goes on, increasing μ implies increasing the security tolerance of the network, leading to wastes of power and time, thereby reducing economic profits. These figures also show that the topology of the power grid does not significantly affect the power blackouts.

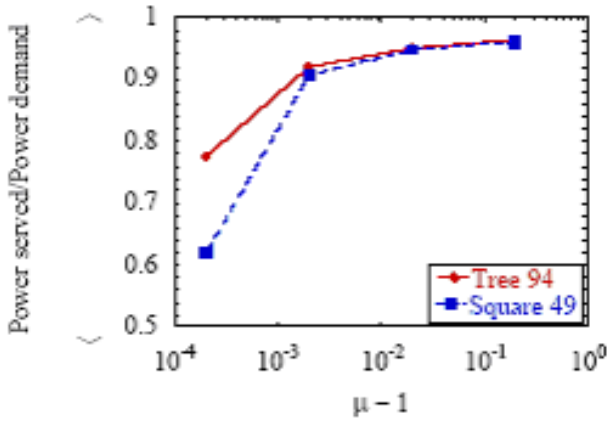


Fig. 6-17 Ratio of power-served and power-demand versus parameter μ [21]

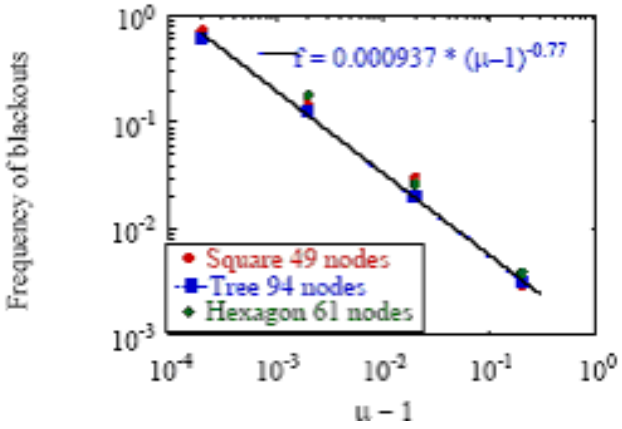


Fig. 6-18 Failure frequency versus parameter μ on different topologies [21]

As power demand increases, power-served on the network will reach the maximum, around which the probability of failures (blackouts) follows a power-law form, and the probability of blackout will increase rapidly, so that in this case the power demand arrives at a threshold value [20].

Power grid blackouts occur typically due to power-served or power-overloading of transmission lines. In the OPA model, these two types of failures correspond to two different thresholds, depending on the operational conditions and the distance between the two threshold values [22]. As the power demand continues to increase, the model has several transition points, representing the changes of the network characters: one is the load shed, in which the power demand cannot be met by the generators due to insufficient capacity or transition line outage; another is the number of line outages. Near a transition point, the probability of failure follows a power law and so it will rapidly increase around the transition point, leading to a sudden change of the power-served, as shown in Fig. 6-19 [22].

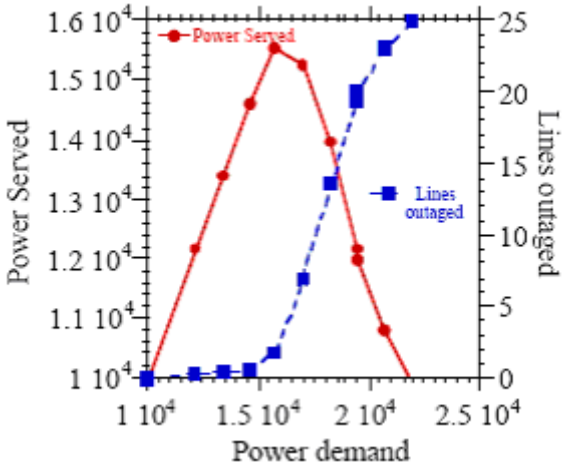


Fig. 6-19 Power served versus power demand in a tree-network of 190 nodes [22]

In a simulation on a power grid model with 382 nodes (12 generator and 370 loads), the loads on nodes were increased in a constant speed. When the loads were increased to 31480MW, the total power of all generators, some nodes started to blackout. If loading keeps increasing, the number of blackout nodes will also increase. When the loading reached 45725MW, some transmission lines reached their capacities thereby causing outages, eventually lead to more node failures, as shown by Fig. 6-20 [22].

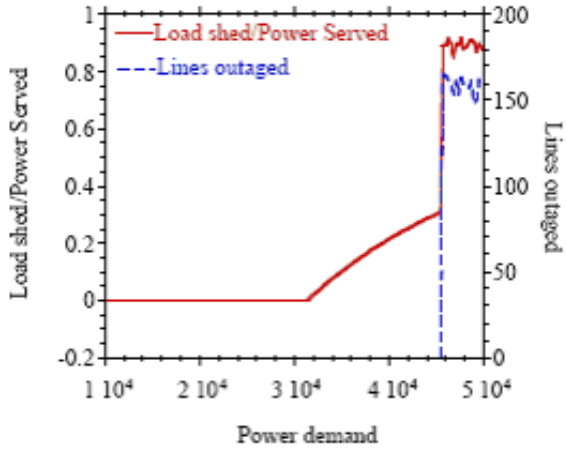


Fig. 6-20 Ratio of load shed over power-served versus power demand in a tree-network of 382 nodes [22]

6.2.7 CASADE Model

From the above discussion on the OPA model, it can be seen that the increase of power loading is the main cause of large-scale blackouts on power grids. In order to better understand the cascading frequency and the distribution of failure probability, the so-called CASCADE model was created [23].

Assume that (i) the network has a large number of nodes of the same type, each has an initial load and initial perturbation; (ii) a node fails when it exceeds the maximum

capacity thereby transferring an amount of load, P, to the other nodes. In this process:

1) all N nodes are initially in the normal state, with initial loads L_1, …, L_N, which are independent random variables uniformly distributed in $[L_{\min}, L_{\max}]$;

2) add the initial disturbance D to each node i, $i = 1,2,...,N$, and set $i \leftarrow 1$;

3) test each node j: if $L_j > L_{fail}$ then node j fails; suppose m_j nodes fail at this step, $j = 1,2,...,N$:

3.1) if $m_j = 0$ then stop, the cascading process ends;

3.2) if $m_j > 0$ then on this node j, do $L_j \leftarrow L_j + m_j P$; set $i \leftarrow i+1$, and return to step 3).

Compared to the OPA model, this CASCADE model is simpler and can be used to study the distribution of cascading failure probability.

Let $f(r,d,p,N)$ be the density function of the probability that r nodes out of N fail, $r < N$, where d is a constant parameter. Then, it can be shown [23] that this density function follows a quasi-binomial distribution:

$$f(r,d,p,N) = \binom{N}{r} d(rp+d)^{r-1}(1-rp-d)^{N-r}, \quad 0 \le r \le (1-d)/p$$

$$f(r,d,p,N) = 0, \quad (1-d)/p < r < N, \quad 0 \le r$$

$$f(n,d,p,N) = 1 - \sum_{s=0}^{N-1} f(s,d,p,N), \text{ otherwise}$$

When $np + d \le 1$, the above three formulas can be combined as

$$f(r,d,p,N) = \binom{N}{r} d(rp+d)^{r-1}(1-rp-d)^{n-r} \tag{6-17}$$

Simulation on a power network model of $N = 1{,}000$, with average node degree $\langle r \rangle$, produces the result shown in Fig. 6-21 [23], where the dark color on the region bounded by the lines $np + d = 1$ (right) and $d = 0$ (up) implies that all nodes have very high probability to fail, where $\langle r \rangle \approx 1{,}000$. On the left-hand side of $np + d = 1$

and the up side of $d = 0$, the colors are lighter, where $f(r, d, p, N)$ satisfies (6-17) and

$$\langle r \rangle = nd \sum_{r=0}^{N-1} \frac{(N-1)!}{(N-r-1)!} p^r$$

which is proportional to parameter d. When d is fixed small, while p is varied, the distribution of $\langle r \rangle$ is shown in Fig. 6-22 [23]. It can be seen that for all p, the probability of having no failures is the same, 0.9. It can also be seen that when $p = 0.0001$, $\langle r \rangle$ follows an exponential distribution; when $p = 0.001$, $\langle r \rangle$ has an near power-law distribution; when $p = 0.002$, there is a singleton up to the value 0.8 at $\langle r \rangle = 1{,}000$, implying that all nodes fail with probability 0.8.

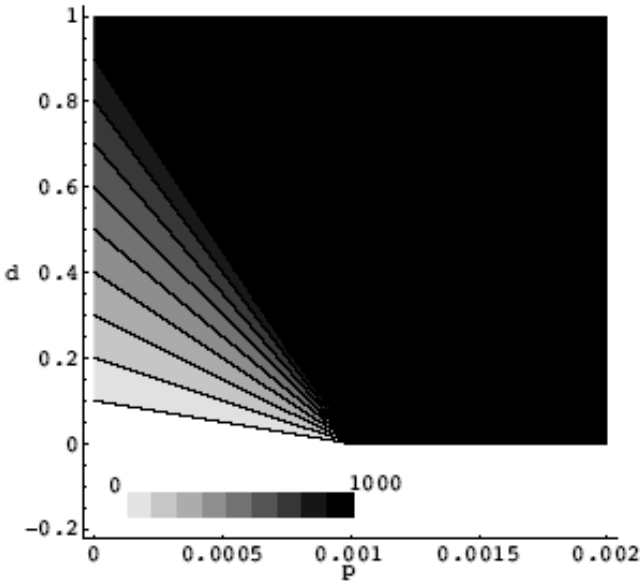


Fig. 6-21 Average failed nodes versus p and d [23]

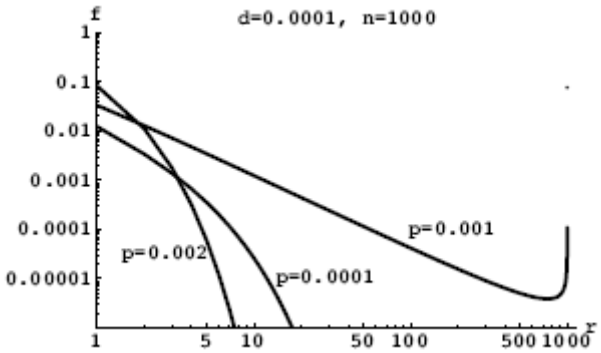


Fig. 6-22 Distribution of $\langle r \rangle$ versus p [23]

Figures 6-23 and 6-24 [24] show the effects of average load L on the failures [24]. It can be seen from Fig. 6-23 hat for the CASCADE model there is a threshold value $L \approx 0.8$ over which failure occurs rapidly. It can also been seen from Fig. 6-24 that the failure probability is 0.61, 0.37, 0.14 when L = 0.6, 0.8, 0.9, respectively. It is clear that when the loading is low, $L = 0.6$, the probability distribution of $\langle r \rangle$ follows an exponential curve, but near the threshold value, $L \approx 0.8$, $\langle r \rangle$ follows a power-law curve, which implies that when the average loading is low, individual node failures are relatively independent, but when the loading exceeds the threshold, it is quite possible that catastrophic cascading failures will occur. This conclusion is consistent with the OPA model.

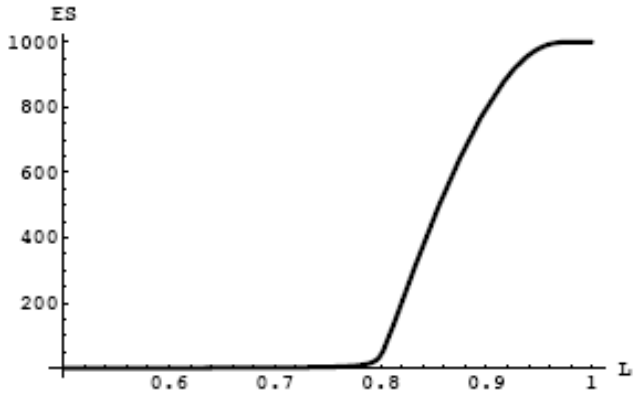


Fig. 6-23 Number of failed nodes ES versus the average load L [24]

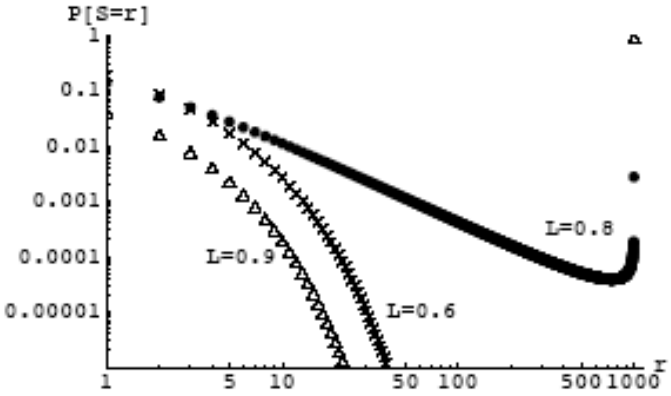


Fig. 6-24 Distribution of average failures $\langle r \rangle$ versus the average load L [24]

6.2.8 Other Models

Cascading reactions or failures over complex networks have been studied under some other models. Representative models include: a fluid model and a birth-death model for router networks [25]; a hybrid differential-algebraic equations model [26], a Monte Carlo model [27] and a Markov-chain model [28] for power networks, etc.

6.3 Cascading Failures in Coupled Map Lattices

Coupled map lattices (CMLs) have been widely investigated over the past decades to model rich spatiotemporal dynamical behaviors of complex systems [29]. Typically, a coupled map lattice is assumed to have a regular coupling (such as global coupling or nearest-neighbor coupling) topology. Recently some dynamical behaviors of CMLs have been investigated, including such as chaos and synchronization on CMLs [30].

6.3.1 Cascading Failure Model Based on CMLs

Consider a CML of N nodes, described by

$$x_i(t+1) = \left| (1-\varepsilon) f(x_i(t)) + \varepsilon \sum_{j=1\&\, j\neq i}^{N} a_{i,j} f(x_j(t))/k(i) \right|, \quad i = 1, 2, ..., N \quad \text{(6-18)}$$

where $x_i(t)$ is the state variable of the ith node at the tth time step, the coupling matrix $A = (a_{ij})_{N\times N}$: if there is an edge between node i and node j then $a_{ij} = a_{ji} = 1$; otherwise, $a_{ij} = a_{ji} = 0$. Clearly, A is a symmetrical 0-1 matrix with zero diagonal elements because self-loops are not allowed. In this model, $k(i)$ denotes the degree of node i, constant $\varepsilon \in (0,1)$ represents the coupling strength, function f defines the local dynamics, which is chosen to be the chaotic logistic map, $f(x) = 4x(1-x)$, in this study. The absolute value is used in the model to guarantee that each state is always nonnegative, for simplicity of analysis.

Node i is said to be in a normal state at the mth time step if $0 < x_i(t) < 1, t \le m$. On the other hand, if $0 < x_i(t) < 1,\ t < m;\ x_i(m) \ge 1$, then node i is said to fail at the mth time step. In this case, assume that $x_i(t) \equiv 0, t > m$. If the initial states of the nodes in network (6-18) all lie in the interval (0, 1) and there are no external perturbations, then the N nodes in the network will be in normal states forever.

In order to show how an initial shock to a single node can trigger cascading failures, an external perturbation $R \ge 1$ is added to a node c at the mth time step, yielding

$$x_c(m) = \left| (1-\varepsilon) f(x_c(m-1)) + \varepsilon \sum_{j=1\&\, j\neq c}^{N} a_{c,j} f(x_j(m-1))/k(c) \right| + R \quad \text{(6-19)}$$

In this case, node c will fail at the m th time step, and so $x_c(t) \equiv 0$ for all $t > m$.

At the $(m+1)$st time step, the states of those nodes that are directly connected with node c will be affected by $x_c(m)$ according to (6-18), and the states of these nodes may also be larger than 1 thus may lead to a new cycle of node failures. The question is: in this scenario, how many nodes will fail eventually?

In the following simulations, the initial states of the nodes in the coupled map lattice (6-18) are all chosen randomly from the interval $(0, 1)$. A perturbation $R \geq 1$ is added to node c at the 10th time step. Cascading failure process can be characterized by the total number of failed nodes in the network before the $(t+1)$st time step, denoted as $I(t)$. Thus, $I = \lim_{t\to\infty} I(t)$ measures the final size of the failures in the network.

6.3.2 Cascading Failures on Typical Coupling Lattices

Globally Coupled Map Lattices

In a globally CML network, each node connects to all the other nodes.

In this simulation, $N = 2{,}000$ and $\varepsilon = 0.6$. After a perturbation $R \geq 1$ is added to a randomly selected node in such a network at the 10th time step, it is found that for any given size N and any coupling strength $\varepsilon \in (0,1)$ of the network, there exist two thresholds, $R_{c1} \equiv R_{c1}(\varepsilon, N)$ and $R_{c2} \equiv R_{c2}(\varepsilon, N)$, with $R_{c1} < R_{c2}$, as shown in Fig. 6-25 [31]. In the simulation, the two thresholds turned out to be $R_{c1} \approx 29.4$ and $R_{c2} \approx 41.4$. Below threshold R_{c1}, i.e., $1 < R \leq R_{c1}$, $I = 1$, implying that there exist no failed nodes in the network. However, as R increases from R_{c1} beyond, the size I of cascading failures increases very rapidly. Once the amplitude R of the perturbation reaches another threshold, R_{c2}, i.e., $R \geq R_{c2}$, all nodes in the network fail, i.e., $I \equiv N$.

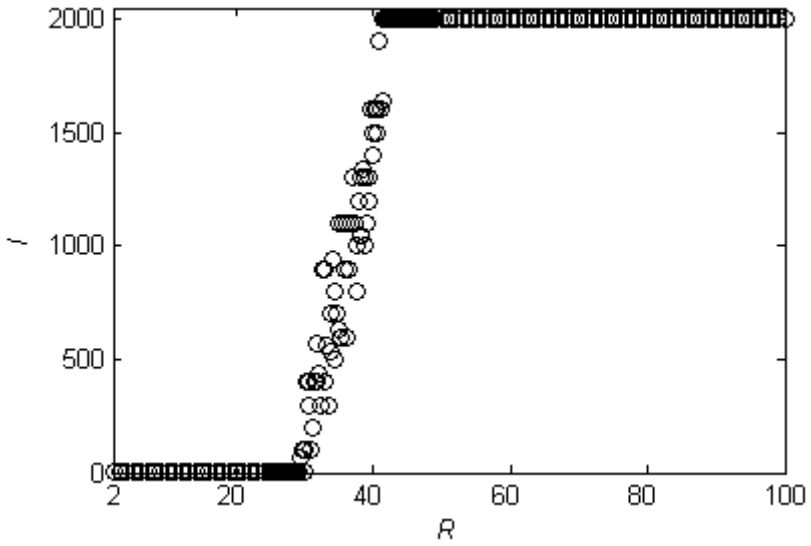


Fig. 6-25 Size of cascading failures I versus perturbation R [31]

Mathematically, the threshold R_{c2} can be estimated as follows. All nodes fail in the $(m+1)$ st time step means that

$$x_i(m+1) = \left| f(x_i(m)) + \frac{\varepsilon}{N-1}\sum_{j=1}^{N}(f(x_j(m) - f(x_i(m)) \right| \geq 1, \quad i \neq c \tag{6-20}$$

Note that

$$f(x_c(m)) = 4x_c(1-x_c) \leq -4R(R-1) \leq 0 \tag{6-21}$$

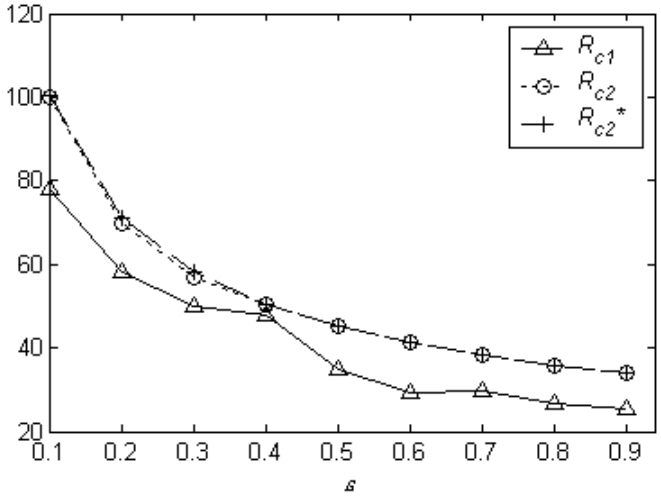
It can be verified that

$$f(x_i(m)) + \frac{\varepsilon}{N-1}\sum_{j=1}^{N}(f(x_j(m) - f(x_i(m)) \leq 1 + \frac{\varepsilon}{N-1}(f(x_c(m) - 1) \tag{6-22}$$

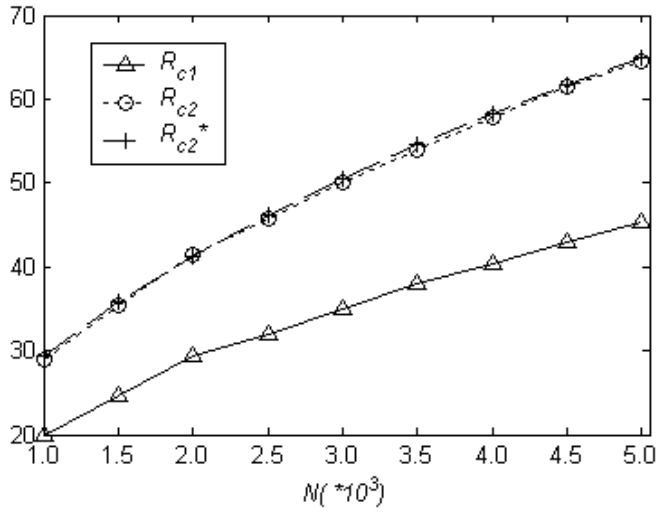
From (6-21) and (6-22), it can be verified that (6-20) holds if

$$R \geq R_{c2}^{*} \equiv \frac{1}{2}\left(1 + \sqrt{\frac{2(N-1)}{\varepsilon}}\right) \tag{6-23}$$

It can be seen from Fig. 6-26 [31] that the threshold R_{c2}^{*} estimated by (6-23) fits very well to the threshold R_{c2} obtained from the simulation, where $N = 2000$ and R_{c1} and R_{c2} are obtained from the data averages over 100 trials.



(a)



(b)

Fig. 6-26 Thresholds for cascading failures in globally coupled map lattices [31]

It should be noted that in the limit as $N \to \infty$, thresholds R_{c1} and R_{c2} increase to infinity. This implies that a large-scale globally CML network is very robust against large but local external perturbations.

Small-World Coupled Map Lattices

Although, in general, globally coupled networks can capture some important features of the corresponding real-world networks, it is easy to see its limitation: a general globally coupled network with N nodes has $N(N-1)/2$ edges, while most large-scale real-world networks actually are sparse; that is, the number of edges in a real network is generally in order of N rather than N^2. This means that globally

coupled network models are unlikely realistic. Instead, small-world networks can provide better models.

Consider a nearest-neighbor coupled network, consisting of N nodes arranged in a ring where each node i is adjacent to $2K$ neighboring nodes, with K being an even integer (Section 3.2, Chapter 3). In simulations, set $K = 20$, $\varepsilon = 0.6$ and $N \geq 1000$. A perturbation $R \geq 1$ is added to a randomly selected node at the m th time step.

It is found that for a large perturbation, $R > 6$, the number of failed nodes before the $(m+t+1)$ st time step is about $I(m+t) = Kt + 1$. Therefore, it requires about N/K time steps for the cascading failures to propagate over all the nodes in the ring, and $N/K \to \infty$ as $N \to \infty$.

It is also found that it is much easier to trigger global cascading failures on a small-world CML than on a nearest-neighboring CML, i.e., a ring. In simulations, set $N = 2000$, $K = 20$, $p = 0.05$ and $\varepsilon = 0.6$. Figure 6-27 [31] shows a plot of the size I of cascading failures, as a function of the amplitude R of the external perturbation, when a randomly selected node failed at the 10th time step caused by the perturbation. It can be seen that all the nodes in the network failed within just a few steps if $R > 5.5$. For example, when $R = 6$, all the nodes in the network failed after 7 steps, as shown in Fig. 6-28 [31]. This implies that a few long-range connections are sufficient for a single node failure to trigger cascading failures in a large-scale network, leading to collapse in just a few steps in this simulation.

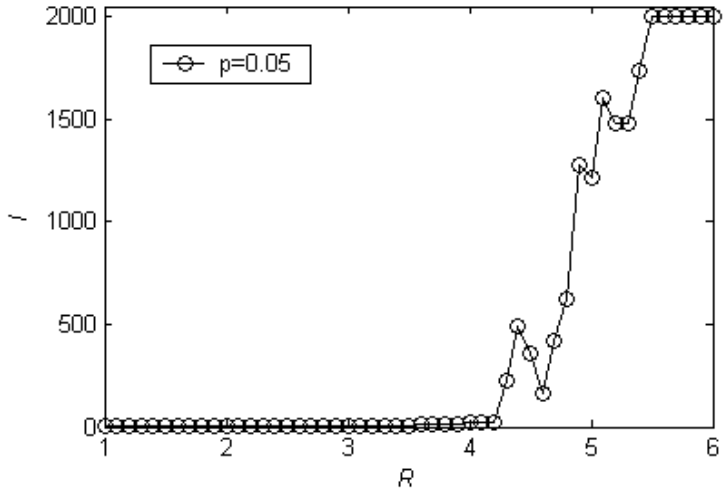


Fig. 6-27 Size of cascading failures I versus perturbation R [31]

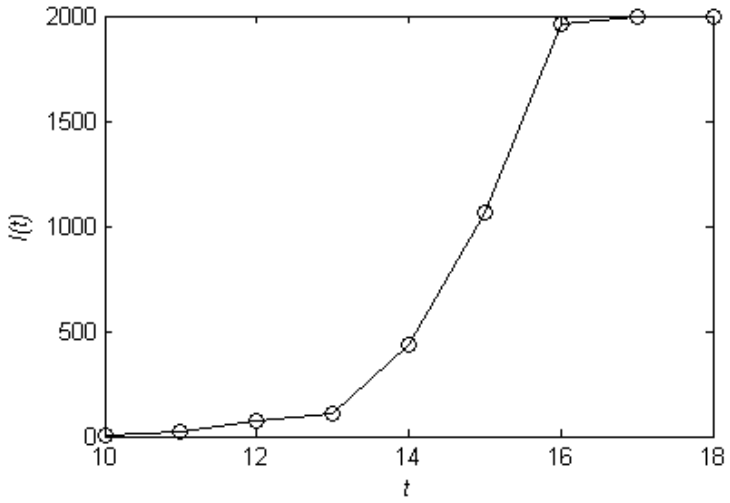
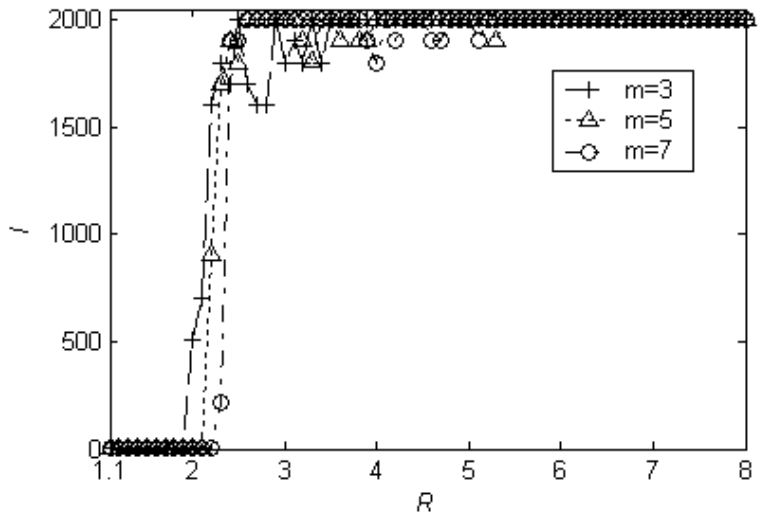


Fig. 6-28 Size of cascading failures I caused by single node failure [31]

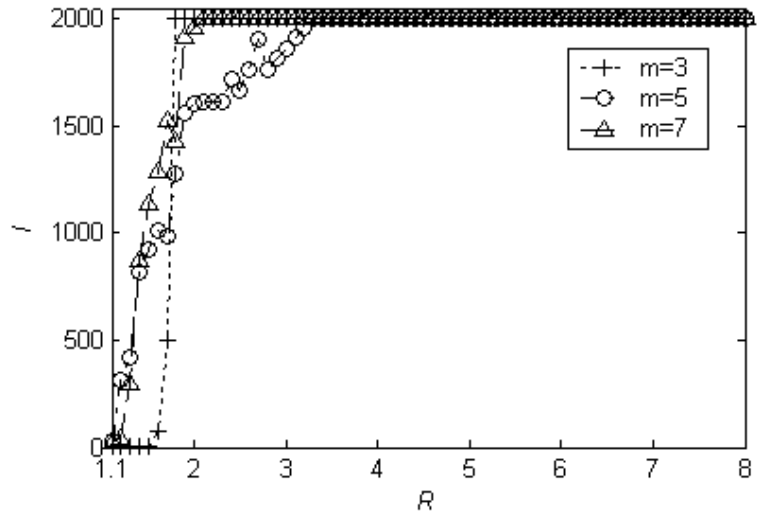
Scale-Free Coupled Map Lattices

In a BA scale-free CML network model, with $N = 2000$ and $\varepsilon = 0.6$, in order to take into account the inhomogeneous feature of the network, two different triggering strategies are adopted: random attack and selective attack. In the random attack, an initial shock is added to a node chosen at random; in the selective attack, an initial shock is added to the node with largest degree in the network.

Figure 6-29 [31] shows the plots of the size of cascading failures as the function of the amplitude R of the perturbation, under (a) random attack and (b) selective attack, respectively. It can be seen that there is no sharp difference in the results between random and selective attacks. In each case, there exists a similar threshold R^*_{BA}. Below the threshold, only a few nodes (less than 10 in this simulation) will fail. As the value of R increases after the threshold, the size I of cascading failures increases very rapidly to the size N of the network. It can also be seen that the threshold R^*_{BA} is much smaller than the threshold R_{c1} for a globally coupled network with the same size N and coupling strength ε. This implies that it is much easier to trigger network collapse in a scale-free network than in a globally coupled network. Figure 6-30 [31] shows the cascading failure process in a scale-free CML with $m = 3$ and $R = 10$.



(a)



(b)

Fig. 6-29 Size of cascading failures I versus perturbation R [31]

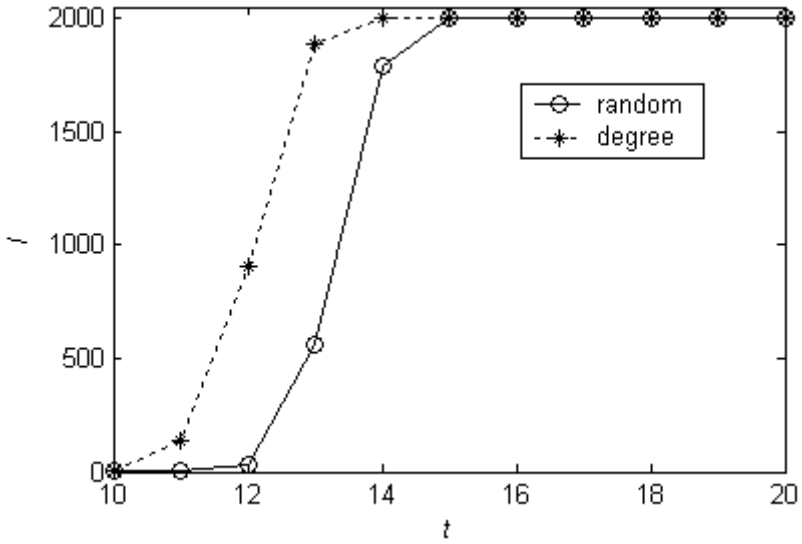


Fig. 6-30 The cascading failure process under random and selective attacks [31]

Next, in order to consider the effects of the exponent γ in the power law $P(k) \sim k^{-\gamma}$ of a scale-free network on the cascading failure propagation, consider a variant of the BA model [33]: Start with N nodes in the network, labeled by i, $i = 1, ..., N$. Assign a weight $p_i = i^{-\alpha}$ to each node i, where $\alpha \in [0,1)$ is a control parameter. Then, select two different nodes i and j with probabilities equal to the normalized weights, $p_i / \sum_k p_k$ and $p_j / \sum_k p_k$, respectively, and add an edge between them, likewise prohibiting self-loops and multiple edges. This process is repeated until mN edges have been added. Thus, the average node degree is $2m$, and the degree distribution follows the power law $P(k) \sim k^{-\gamma}$ with $\gamma = 1 + \frac{1}{\alpha}$. By adjusting the control parameter α, various exponents γ can be obtained in the interval $(2, +\infty)$.

To understand the effect of the exponent λ on some topological properties of the network model, construct different scale-free networks with $N = 3{,}000$ and the control parameter α varying from 5/6 to 1/9, corresponding to the variation of exponent γ from 2.2 to 10. It is found that the number of nodes contained in the largest connected sub-net varies from 2,938 to 3,000. Notice that the degree distribution of the network with $\gamma = 10$ is approximately equal to that of a random-graph network. Figure 6-31 [32] shows a plot of the largest degree $K_{\max}$ and average distance D_{avg} of a scale-free network as a function of the exponent γ. It is clear that a smaller γ leads to a larger $K_{\max}$ and a smaller D_{avg}. In other words, as the value of exponent γ decreases, the network becomes more heterogeneous, with a smaller connected sub-net.

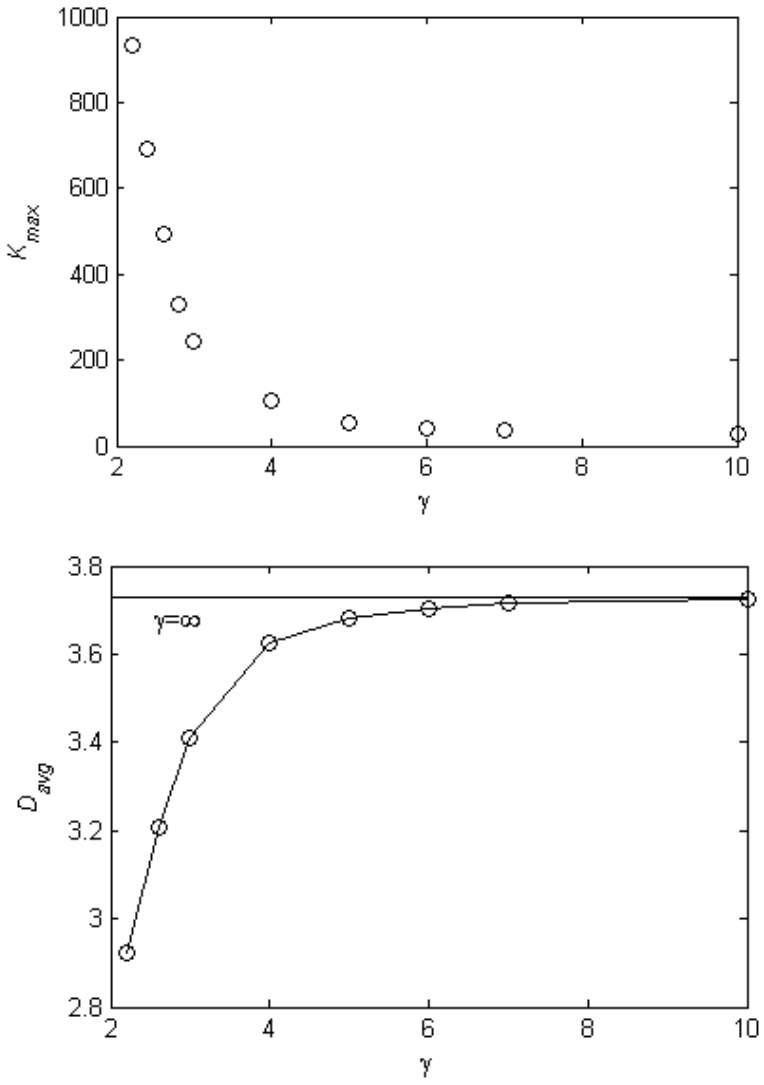
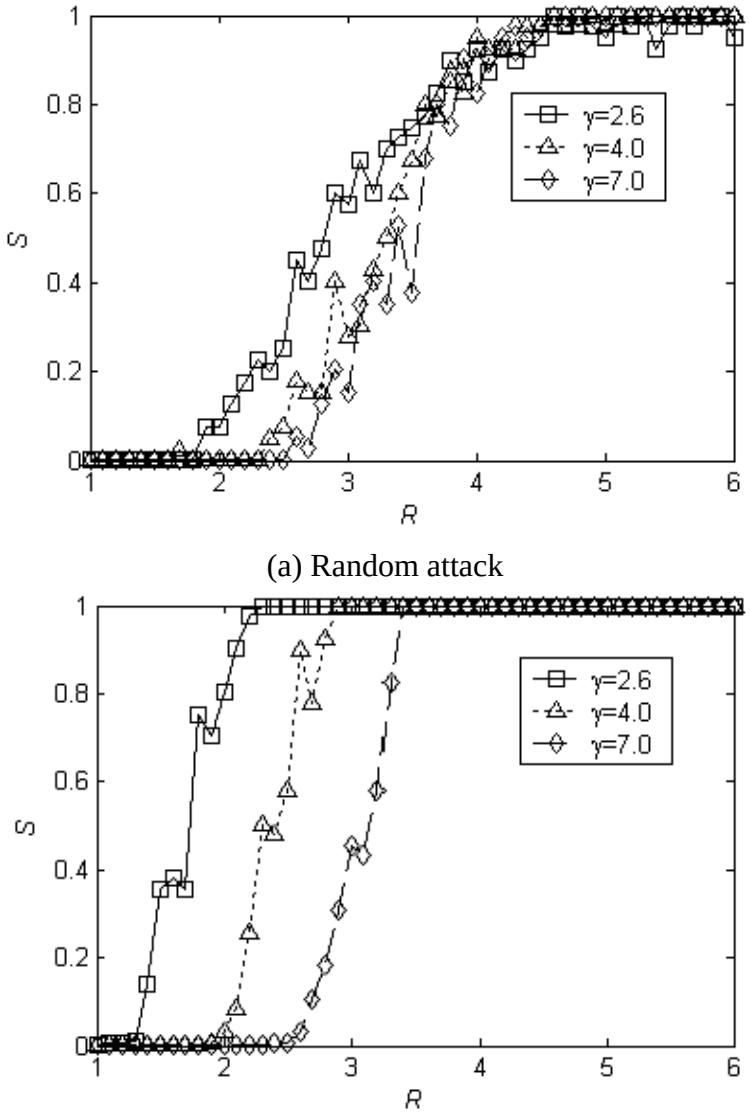


Fig. 6-31 The largest degree $K_{\max}$ and average distance D_{avg} versus γ [32]

Next, to see the effect of the exponent γ on the cascading failures over the scale-free networks, similarly two different strategies are adopted to trigger cascading reactions on a scale-free CML model: random attack and selective attack. In the random attack, an initial perturbation $R \geq 1$ is added to a node chosen at random; in the selective attack, the perturbation is added to the node with the largest degree in the network.

In simulations, set $m = 5$ and $\varepsilon = 0.6$. The relative size of cascading failures is defined as $S = I / N$, where I is the total number of failed nodes in a network. Figures 6-32 (a) and (b) [32] show a plot S as a function of the amplitude of the disturbance R, in the cases of $\gamma = 2.6$, 4 and 7, under random attack and selective attack, respectively. It can be seen that in each case, there exists a threshold, R_c,

below which only a few nodes (less than 5%) failed. As the value of R increases after the threshold, the size of cascading failures increases rapidly to near 100%, i.e., the entire network fails.



(a) Random attack

(b) Selective attack

Fig. 6-32 Size of cascading failures versus exponent γ [32]

Figure 6-33 [32] shows a plot of the threshold R_c as a function of γ. It can be seen that in both random and selective attacks, the threshold R_c for cascading failures is an increasing function of γ. This implies that as the network becomes more homogeneous, the network becomes more robust against both random and selective attacks. In other words, as the network becomes more heterogeneous, the network becomes more vulnerable to both random and selective attacks. This could attribute to

the small-world feature of scale-free networks: As the exponent γ decreases, the heterogeneity of the network increases and the average distance of the network decreases. Therefore, it may be easier for an initial perturbation to spread out over a higher heterogeneous network. This is consistent with the analysis of virus spreading studied in Chapter 5.

It can also be seen from Fig. 6-33 that, for a fixed exponent γ, i.e., for a network with fixed heterogeneity, the threshold for cascading failures under selective attack is smaller than that under random attack, especially when $\gamma \le 3$. This implies that it is much easier for cascading failures to emerge in a higher heterogeneous network under selective attack than random attack. This is reasonable because in a higher heterogeneous network, nodes with larger degrees always take on larger loads and they play a more important role in the stability of the network.

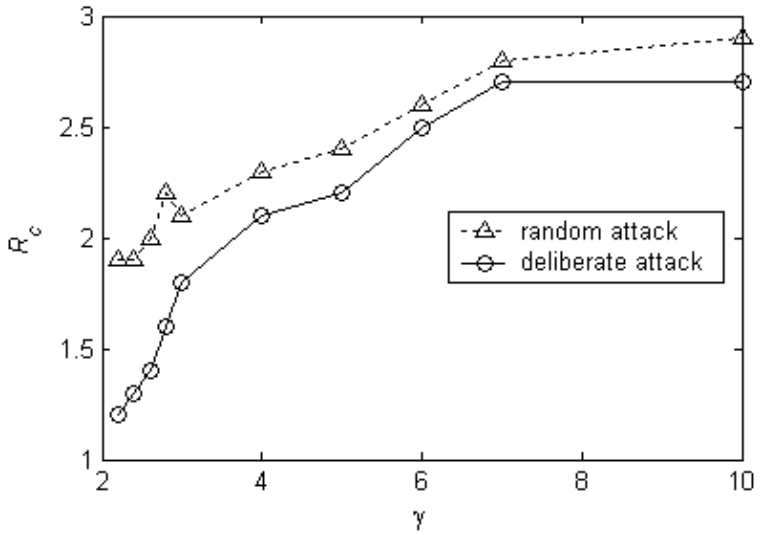


Fig. 6-33 Threshold R_c versus exponent γ [32]

Finally, Fig. 6-34 [32] shows the cascading failure process in a scale-free CML with $\gamma = 3$, triggered by an initial perturbation $R = 6$. In the selective attack case, the network collapses within 4 time steps, while in the random attack case, it collapses within 6 time steps.

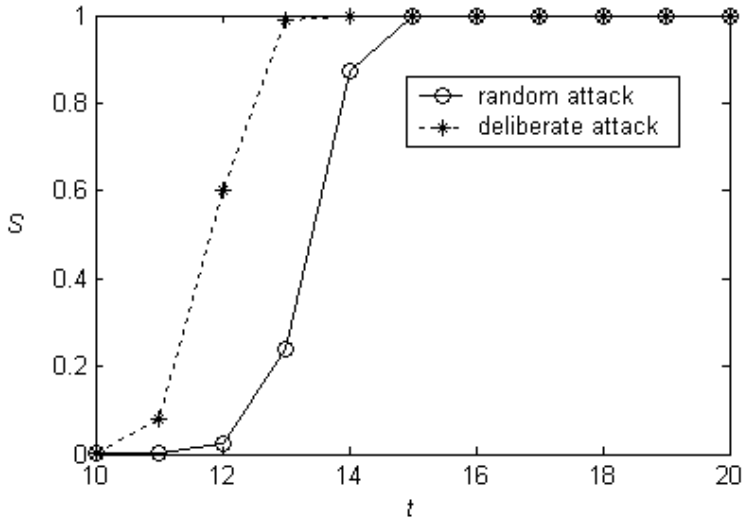


Fig. 6-34 Size of cascading failures in a scale-free CML with $\gamma = 3$ [32]

References

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

[2] Motter A E, Nishikawa T, Lai Y-C. Cascade-based attacks on complex networks. *Phys. Rev. E*, 2002, 66: 065102(R)

[3] http://moat.nlanr.net/AS/Data/ASconnlist.20000102.946809601

[4] Holme P, Kim B J, Yoon C N, Han S K. Attack vulnerability of complex networks. *Phys. Rev. E*, 2002, 65: 056109

[5] Moreno Y, Pastor-Satorras R, Vázquez A, Vespignani A. Critical load and congestion instabilities in scale-free networks. *Europhys. Lett*., 2003, 62: 292-298

[6] Holme P, Kim B J. Vertex overload breakdown in evolving networks. *Phys. Rev. E*, 2002, 65: 066109.

[7] Crucitti P, Latora V, Marchiori M. Model for cascading failures in complex networks. *Phys. Rev. E*, 2004: 69, 045104(R)

[8] Albert R, Albert I, Nakarado G L. Structural vulnerability of the North American power grid. *Phys. Rev. E*, 2004, 69: 025103(R)

[9] Kinney R, Crucitti P, Albert R, et al. Modeling cascading failures in the north American power grid. 2004, cond-mat/0410318

[10] Carreras B A, Lynch V E, Newman D E, et al. Blackout mitigation assessment in power transmission systems. *Proceedings of 34th Hawaii International Conference on System Science*, 2001, 1-9

[11] Carreras B A, Newman D E, Dolrou I, et al. Initial evidence for self-organized criticality in electric power system blackouts. *Proceedings of 33th Hawaii International Conference on System Sciences*, 2000, 1-6

[12] Asavathiratham C. *The Influence Model: A Tractable Representation for the Dynamics of Networked Markov Chains* [Dissertation], Elec. Eng. and Comp. Sci. Dept., MIT, 2000

[13] Watts D J. A simple model of global cascades on random networks. *Proc. Natl. Acad. Sci. U.S.A.*, 2002, 99: 5766-5771

[14] Bak P, Tang C, Wiesenfeld K. Self-organized criticality: An explanation of the 1/f noise. *Phys. Rev. Lett.*, 1987, 59: 381-384

[15] Bonabeau E. Sandpile dynamics on random graphs. *J. Phys. Soc. Japan*, 1995, 64: 327-328

[16] Lise S, Paczuski M. Nonconservative earthquake model of self-organized criticality on a random graph. *Phys. Rev. Lett.*, 2002, 88: 228301

[17] Olami Z, Feder H J S, Christensen K. Correlation functions in the fully frustrated 2D XY model. *Phys. Rev. Lett.*, 1992, 68: 1224-1227

[18] Lee D-S, Goh K-I, Kahng B. et al. Sandpile avalanche dynamics on scale-free networks. *Physica A*, 2004, 338: 84-91

[19] Goh K-I, Lee D-S, Kahng B, et al. Sandpile on scale-free networks. *Phys. Rev. Lett*, 2003, 91: 148701

[20] Dobson I, Chen J, Thorp J S, Carreras B A, Newman D E. Examining criticality of blackouts in power system models with cascading events. *Proceedings of 35th Hawaii International Conference on System Sciences*.2002, 63-72

[21] Carreras B A, Lynch V E, Dobson I, Newman D E. Dynamics, criticality and self-organization in a model for blackouts in power transmission systems. *Proceedings of 35th Hawaii International Conference on System Sciences*. 2002, 1-8

[22] Carreras B A, Lynch V E, Dobson I, et al. Critical points and transitions in an electric power transmission model for cascading failure blackouts. 2002, *Chaos*, 12 (4): 985-994

[23] Dobson I, Carreras B A, Newman D E. A probabilistic loading-dependent model of cascading failure and possible implications for blackouts. *Proceedings of 35th Hawaii International Conference on System Sciences*. 2003, 1-8

[24] Dobson I, Carreras B A, Newman D E. A loading-dependent model of probabilistic cascading failure. *Probability in the Engineering and Informational Sciences*, 2005, 19 (1): 15-32

[25] Coffman Jr E G, Ge Z, Misra V, et al. Network resilience: Exploring cascading failures within BGP. *Proceedings of the 40th Annual Allerton Conference on Communications, Computing and Control.* 2002, 1-10

[26] Parrilo P A, Lall S, Paganini F, et al. Model reduction for analysis of cascading failures in power systems. *Proceedings of the American Control Conference*, 1999, 6: 4208-4212

[27] Rios M A, Kirschen D S, Jawayeera D, et al. Value of security: modeling time-dependent phenomena and weather conditions. *IEEE Transactions on Power Systems*, 2002, 17(3): 543-548

[28] Pepyne D L, Panayiotou C G, Cassandras C G. Vulnerability assessment and allocation of protection resources in power systems. *Proceedings of the American Control Conference*, 1999, 6: 4705-4710

[29] Kaneko K. *Coupled Map Lattices.* Singapore: World Scientific, 1992

[30] Gade P M, Hu C-K. Synchronous chaos in coupled map lattices with small-world interactions. *Phys. Rev. E*, 2000, 62: 6409-6413

[31] Wang X F, Xu J. Cascading failures in coupled map lattices. *Physical Review E*, 2004, 70: 056113.

[32] Xu J, Wang X F. Cascading failures in scale-free coupled map lattices. *Physica A*, 2005, 349: 685-692

[33] Goh K-I, Kahng B, Kim, D. Universal behavior of load distribution in scale-free networks. *Phys. Rev. Lett.* 2001, 87: 278701

