Available online at www.sciencedirect.com
SCIENCE DIRECT®
Physica A 340 (2004) 388–394
PHYSICA A
www.elsevier.com/locate/physa

Error and attack tolerance of complex networks

Paolo Crucitti[a,*], Vito Latora[b], Massimo Marchiori[c,d], Andrea Rapisarda[b]

[a] *Scuola Superiore di Catania, Via S. Paolo 73, 95123 Catania, Italy*
[b] *Dipartimento di Fisica e Astronomia, Università di Catania, and INFN sezione di Catania, Corso Italia 57, 95129 Catania, Italy*
[c] *W3C and Laboratory for Computer Science, Massachusetts Institute of Technology, USA*
[d] *Dipartimento di Informatica, Università di Venezia, Italy*

Abstract

Communication/transportation systems are often subjected to failures and attacks. Here we represent such systems as networks and we study their ability to resist failures (attacks) simulated as the breakdown of *a group of nodes* of the network chosen at random (chosen accordingly to degree or load). We consider and compare the results for two different network topologies: the Erdös–Rényi random graph and the Barabási–Albert scale-free network. We also discuss briefly a dynamical model recently proposed to take into account the dynamical redistribution of loads after the initial damage of *a single node* of the network.

PACS: 89.75.−k; 89.75.Fb; 05.90.+m

Keywords: Structure of complex networks; Scale-free networks

1. Introduction

Most of the communication/transportation systems of the real world can be represented as complex networks, in which the *nodes* are the elementary components of the system and the *edges* connect pair of nodes that mutually interact exchanging information. To quote a few examples: in the Internet the nodes are the routers and the edges (or arcs) are the cables connecting couples of routers; in an electrical power grid the nodes are the substations (generators or distribution substations) and the edges are the transmission lines; in a city road system the nodes are the crossings and the

* Corresponding author. Fax: +39-095-361-054.
E-mail address: pacrucitti@ssc.unict.it (P. Crucitti).

0378-4371/$ - see front matter
doi:10.1016/j.physa.2004.04.031

edges are the roads; and in transportation systems considered on a larger scale, the nodes are the cities and the edges are the highways or the flights connecting a couple of cities. In the last few years the accessibility of large databases of technological and also biological networks has made possible a series of empirical studies to characterize the connectivity properties of such networks [1,2].

One of the most important and unexpected results found in the literature is that technological networks such as the World Wide Web [3,4], the Internet [5]), airplanes connection networks [6], and some biological systems, as metabolic networks [7] and protein–protein networks [8], are different from random networks [9] and all share the same property of having a *power-law degree distribution* $P(k) \sim k^{-\gamma}$ with an exponent γ that ranges between 2 and 3 [1]. The degree of a node is the number of first neighbours (the number of edges adjacent to the node), and is one of the most commonly used measures of nodes centrality [11]. The degree distribution is the collection of the nodes degree. Networks with power-law degree distribution have been named scale-free networks, and are extremely heterogeneous [10].

Recently, enormous interest has been devoted to the study of the effects of errors and attacks both on scale-free models and on real-world networks [12–17]. The reason for studies on the network tolerance against errors and attacks has to be found in two main goals:

(1) designing new networks as systems well integrated in their environment, taking into account whether only errors or both errors and attacks can occur;
(2) protecting existing networks, locating the most critical nodes and taking counter-measures in order to reduce their criticality.

In Section 2 of this paper we consider the network as an undirected and unweighted graph [1] and we present a *static analysis* of error and attack tolerance for two different model topologies:

- The Erdös–Rényi (ER) random graph [9]: it is constructed starting from an initial condition of N nodes and no edges and then adding K edges between pairs of randomly selected nodes. Under the assumption of sparseness ($K \ll N^2$), it shows a Poissonian degree distribution.
- The Barabási–Albert (BA) scale-free network [3,4]: it starts from an initial condition of a few nodes and then, for each time step, evolves adding a new node (growing) that is connected more likely to nodes with higher degree (preferential attachment). It shows a power-law degree distribution $P(k) \sim k^{-\gamma}$ with $\gamma = 3$.

By *error or failure* we mean the removal of randomly selected nodes. Instead, we call *attack* the targeted removal of the most important nodes. We will consider three different criteria to determine the importance of a node (the first criterium has already

[1] The formalism can be easily extended to the case of directed and weighted networks [18,19]. In Section 3 we will need to consider a weighted network.

been adopted in Ref. [13]:

- the *degree*, i.e., the number of edges the node has;
- the betweenness, or *load* of the node, i.e., the number of shortest paths (over all pairs of nodes of the network) that pass through the node, evaluated before any removal is performed;
- the recalculated betweenness, or *recalculated load*, i.e., the same quantity as the previous one except that shortest paths are recalculated every time a node is removed.

In order to evaluate how well a system works before and after the removal of a set of nodes we use the *global efficiency*, a measure introduced in Ref. [18]. We assume that the network is described by an adjacency matrix whose entry τ_{ij} is 1 if there is an edge joining vertex i to vertex j, and $+\infty$ otherwise. τ_{ij} can be considered as the time it takes to send a unit packet of information along the edge between i and j. If there is no edge between i and j the two nodes communicate through other nodes by using the fastest path. t_{ij} is the time it takes to send a unit packet of information through the fastest path. For instance, in Fig. 1 the shortest path connecting nodes 1–4 is that passing through nodes 6 and 5. It follows that $t_{14} = \tau_{16} + \tau_{56} + \tau_{45}$.

The global efficiency of the network is defined as the average of the efficiency $\varepsilon_{ij} = 1/t_{ij}$ over all couples of nodes [18]:

$$E(\mathbf{G}) = \frac{\sum_{i \neq j \in \mathbf{G}} \varepsilon_{ij}}{N(N-1)} = \frac{1}{N(N-1)} \sum_{i \neq j \in \mathbf{G}} \frac{1}{t_{ij}}. \tag{1}$$

Unlike the characteristic path length, the efficiency E has shown to be a well-defined quantity also for non-connected graphs [18,13].

In Section 3 we will briefly discuss a *dynamical model* recently proposed in Ref. [17]. Such a model is based on the existence of a maximum load that each node can handle and is able to explain the cascading failures observed in some real world network as the Internet.

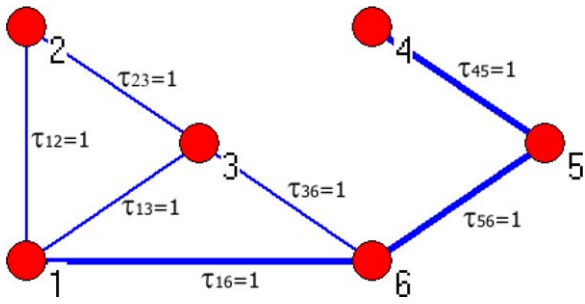

Fig. 1. A simple network made up of $N = 6$ nodes and $K = 7$ edges. The shortest path connecting nodes 1–4 is highlighted.

2. Error and attack tolerance

The malfunctioning of one or more nodes in a network in general affects both the global and the local properties [13] of the remaining nodes, because it makes some edges unusable and consequently, excludes some paths that, before the malfunctioning, contributed to the connectivity of the system. In the following we will only focus on the global properties.

In Fig. 2 we plot the efficiency for the BA scale-free model and for the ER random graph (both with $N=2000$ nodes and $K=10000$ edges) as functions of the percentage p of removed nodes. We compare random removals (errors) with degree-based attacks, i.e., attacks performed removing nodes with the highest number of edges. The BA model shows highly different behaviour with respect to attacks and errors: if we remove 15% of nodes in a targeted way, the network efficiency is reduced to about half the initial value (0.33) and it is sufficient to remove 35% of nodes in order to destroy completely the system; instead, when we remove nodes in a random way, the network efficiency shows a very slow monotonic descendent curve and also for the high value of $p = 80\%$ the system maintains a considerable efficiency, $E = 0.15$.

This behaviour is rooted in the heterogeneity of the scale-free model in which few nodes are responsible for the interconnectedness of the network: their removal causes a rapid drop in the capability of communicating in the system.

As far as the ER graph is concerned, differences of tolerance to attacks and to errors are much less pronounced. In this case, in fact, there is not a substantial variability in the degree: the removal of a node in a targeted or in a random way produces similar, though not equal, behaviours.

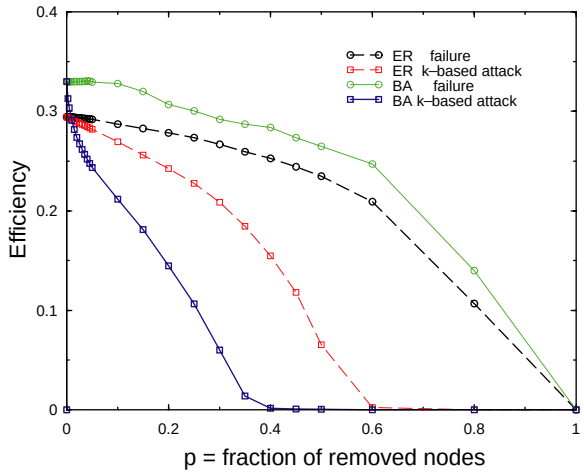

Fig. 2. Error and attack tolerance of BA scale-free graphs and ER random graphs. In both the cases we start with two graphs with $N = 2000$ nodes and $K = 10\,000$ edges and we remove a fraction p of the nodes simulating errors (empty circles) and degree-based attacks (empty squares). We plot the global efficiency E as a function of the percentage p of the nodes removed from the system.

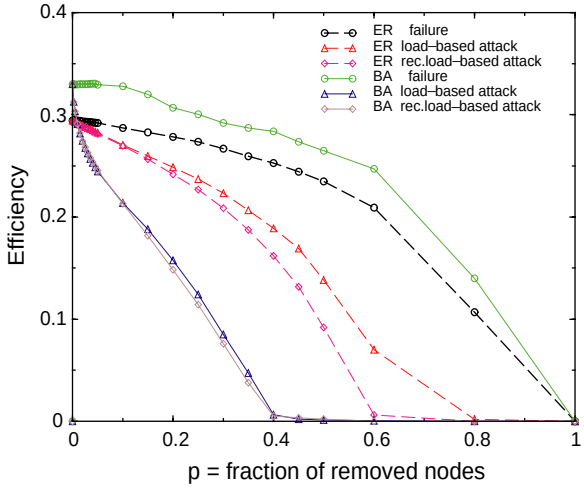

Fig. 3. Error and attack tolerance of BA scale-free graphs and ER random graphs. In both cases we start with two graphs with $N = 2000$ nodes and $K = 10\,000$ edges, and we remove a fraction p of the nodes simulating errors (empty circles), load-based attacks (empty triangles) and recalculated-load-based attacks (empty diamonds). We plot the global efficiency E as a function of the percentage p of nodes removed from the system.

In Fig. 3 we plot again the efficiency for the BA and ER model as a function of p. This time we consider attacks based on the betweenness (recalculated or not) and we compare them with errors, as before. The curves concerning the recalculated-load-based attacks for the BA model do not differ substantially from those relating to degree-based attacks in Fig. 2. Larger differences are visible in the ER graph, for which the recalculated-load-based attack causes a greater amount of damage than the degree-based attack. This is due to the fact that in the BA model many nodes with the highest load are also those with the highest degree, while in the ER model there is not a perfect parallel among load and degree. A different tolerance to recalculated and non-recalculated-load-based attacks is also evident for the ER model: it means that load redistributes over the networks after removal, i.e., when an attack is performed, shortest paths (and consequently load) that passed through the removed nodes are not redistributed in a uniform way and therefore nodes with low betweenness may become those that carry the highest load.

The main conclusion of the static analysis presented in this section is that ER random graphs, due to their homogeneity, exhibit a similar tolerance with respect to errors and attacks, while BA scale-free networks, because of their heterogeneity, are fairly robust to errors, though very vulnerable to attacks.

3. A load redistribution-based model

A question comes out naturally from the static analysis presented in the previous section. Does the load redistribution affect the efficiency of real-world networks? In

other words, are all nodes able to tolerate a high load, although in the absence of attacks they should have carried only a small load? We illustrate such a question with a simple example in which we consider a city road system in which nodes are the crossings, arcs are the streets and the arcs' weights are times τ_{ij} it takes to go from the node i to j following that arc/street. This time we assume $\tau_{ij} > 0 \forall i, j$. If one of the main crossings is interrupted (due to an attack, or simply due to an unlucky failure), drivers who should have passed from that crossing will have to find alternative paths. It is realistic to suppose that the drivers have a perfect knowledge of the state of the system and, therefore, among all the possible remaining paths they will choose the fastest route (if it exists). Unfortunately, after load redistribution, some crossings will not be able to carry the overload and will become congested: the flow of traffic will slow down in all the streets converging to congested crossings, i.e., times τ_{ij} will be degraded. Due to such a slowdown, those which were selected as fastest routes may no longer have this property and a new search for shortest paths begins. The latter will again cause load redistribution, congestion in new crossings and thus new degradation in time. If the overload caused by the interruption of a crossing is small, time degradation will be evident only in a tiny fraction of streets, while if the overload to be reabsorbed is large it will propagate over the whole system with a cascading effect, preventing any efficient communication.

In a recent paper [17] we developed a simple dynamical model that takes into account such a cascading effect. Under the usual assumption that each node sends information (cars) to all the other nodes we determine the shortest paths over all pairs of nodes and we associate each node i with a capacity C_i directly proportional to the initial load/betweenness it has to carry [15]:

$$C_i = \alpha L_i(0) \quad i = 1, 2, \ldots, N. \tag{2}$$

Here $\alpha \geqslant 1$ is a tolerance parameter of the network and $L_i(0)$ is the load handled by the node i at time 0. Eq. (2) is a realistic assumption because the capacity is limited by cost: it would be a waste to build very large and functional crossings in a suburban zone that does not have to carry a high load. Initially the system is in a stationary state with arcs' weights equal to $\tau_{ij}(0)$. The malfunctioning of one or more nodes changes the shortest paths and also the load distribution. If the load of a node i exceeds its capacity, communication involving that node will be degraded and we represent this effect by varying all the arcs' weights τ_{ij} as follows:

$$\tau_{ij}(t+1) = \begin{cases} \tau_{ij}(0)\,\dfrac{L_i(t)}{C_i} & \text{if } L_i(t) > C_i \\ \tau_{ij}(0) & \text{if } L_i(t) \leqslant C_i, \end{cases} \tag{3}$$

where j extends to all the first neighbours of i. In other words, when a node i is congested, we assume that the time to go from (to) i to (from) its first neighbours grows linearly with the overload $(L_i(t))/C_i$.

The numerical simulations of the model [17] have shown the existence of a wide range of the tolerance parameter α for which a BA scale-free network: (1) is resistant to the removal of *a single* randomly chosen node; (2) is not resistant to the removal

of *a single* node chosen among the most important ones. In fact the initial break-up of a node with an extremely large initial load is sufficient to generate a cascading effect that involves the whole network.

Many communication/transportation networks, such as the Internet [17] behave in a similar way: failures occur very frequently in the real world, but we perceive only those caused by the breakdown of critical nodes, while all the others remain confined to limited regions and do not affect the global properties of the system.

4. Conclusions

In this paper we have shown how the topology of a communication/transportation network may have important consequences on error and attack tolerance of the system. In fact, ER random graphs, due to their homogeneity, exhibit a similar tolerance with respect to errors and attacks, while BA scale-free networks, because of their heterogeneity, have turned out to be fairly robust to errors although very vulnerable to attacks. Many real-world networks have scale-free properties and therefore great effort is necessary in order to protect them from attacks.

In the last part of this paper, we have briefly discussed a dynamical approach to the problem based on modelling cascading failures on the networks [17]. Such a simple model explains how the malfunctioning of a single component of a real system can generate a cascading effect, thus causing the entire network to collapse.

References

[1] S.N. Dorogovtesev, J.F.F. Mendes, Evolution of Networks, Oxford University Press, Oxford, 2003.
[2] S.H. Strogatz, Exploring complex networks, Nature 10 (2001) 268.
[3] R. Albert, H. Jeong, A.-L. Barabási, Nature 401 (1999) 130.
[4] A.-L. Barabási, R. Albert, Science 286 (1999) 509.
[5] M. Faloutsos, P. Faloutsos, C. Faloutsos, Comput. Comm. Rev. 29 (1999) 251.
[6] W. Li, X. Cai, cond-mat/0309236.
[7] H. Jeong, B. Tombor, R. Albert, Z.N. Oltvai, A.-L. Barabási, Nature 407 (2000) 651.
[8] H. Jeong, S.P. Mason, A.-L. Barabási, Z.N. Oltvai, Nature 411 (2001) 41.
[9] P. Erdös, A. Rényi, Publ. Math. 6 (1959) 290.
[10] R. Albert, A.-L. Barabási, Rev. Mod. Phys. 74 (2002) 47.
[11] S. Wasserman, K. Faust, Social Networks Analysis, Cambridge University Press, Cambridge, 1994.
[12] R. Albert, H. Jeong, A.-L. Barabási, Nature 406 (2000) 378;
R. Albert, H. Jeong, A.-L. Barabási, Correction, Nature 409 (2001) 542.
[13] P. Crucitti, V. Latora, M. Marchiori, A. Rapisarda, Physica A 320 (2003) 622.
[14] P. Holme, B.J. Kim, Phys. Rev. E 65 (2002) 066109.
[15] A.E. Motter, Y. Lai, Phys. Rev. E 66 (2002) 065102(R).
[16] Y. Moreno, R. Pastor-Satorras, A. Vásquez, A. Vespignani, Europhys. Lett. 62 (2003) 292.
[17] P. Crucitti, V. Latora, M. Marchiori, cond-mat/0309141 and Phys. Rev. E 69 (2004) 045104 (R).
[18] V. Latora, M. Marchiori, Phys. Rev. Lett. 87 (2001) 198701.
[19] V. Latora, M. Marchiori, Europ. Phys. J. B 32 (2003) 249.