Effect of random failures on traffic in complex networks

Jordi Duch[†] and Alex Arenas[†]

[†]Departament d'Enginyeria Informàtica i Matemàtiques,
Universitat Rovira i Virgili, 43007 Tarragona, Spain

ABSTRACT

We study the effect of random removal of nodes in networks on the maximum capability to deliver information in communication processes. Measuring the changes on the onset of congestion, we observe different behaviors depending on the network structure, governed by the distribution of the algorithmic betweenness (number of paths traversing a node given a communication protocol) of the nodes, and particularly by the node with the highest betweenness. We also compare the robustness of networks from a topological and dynamical point of view. We find that for certain values of traffic load, after suffering a random failure, the network can be physically connected but the nodes are unable to communicate due congestion. These results highlight the necessity to include dynamical considerations in studies about resilience of complex networks.

Keywords: Complex Networks, Congestion, Percolation, Robustness

1. INTRODUCTION

Many real complex networks display a high robustness against random failures.[1] This phenomenon has been successfully related to their scale-free degree distribution;[2,3] with a very high probability the random failures will affect the lowest connected nodes, which have small influence in maintaining its structural properties.[4] However, the same degree distribution is also responsible of the vulnerability of scale-free networks against directed attacks (removal of the most connected nodes).[5] Several studies have covered the incidence of removing nodes on the statistical properties of complex networks, such as the diameter,[1] the average path length[3,6] or the size of the giant component.[1,7] Since these properties play an important role in the interplay between the topology and dynamics of complex networks, the node removal will also change the dynamical processes supported on the network.[8]

One of the properties that is affected by the removal of nodes is the *efficiency* of nodes to distribute traffic in communication processes.[9–11] The efficiency between nodes i and j is defined as the inverse of the shortest path connecting them. This property, related to the information flow in networks, is interesting because it allows to quantitatively compare the dynamical performance in traffic of different network structures, however, it obviates one of the most important aspects of any communication process: congestion. In real networks, each node has a limited capability to deliver information, meaning that they can serve a bounded number of "packets" of information per unit time. When the incoming traffic exceeds this capability, the system enters a congested state, there is no balance between incoming and outcoming traffic, and the communication processes become inefficient.[12] A typical example of the effects of such a breakdown is found in power grid networks. The removal of a certain fraction of nodes triggers a cascade failure on the system.[13,14] This failure is caused by the redistribution of the traffic flow between the remaining nodes, surpassing their capability and therefore collapsing some of them.

Aimed by these findings, we propose to study the effect of random breakdowns on the maximum capability of a network to distribute traffic, analyzing the behavior of the congestion point. We have simulated random failures in three different types of networks (regular, Erdos-Renyi and scale-free), using two different routing protocols: shortest paths and random walks. The results of the study show that: (i) random breakdowns in scale-free networks systematically increase the capability of the network to deliver information, independently

on the routing protocol being shortest path or random, (ii) in regular networks the behavior is the opposite random breakdowns decrease the capability of the network to deliver information, independently on the routing protocol being shortest path or random, (iii) in Erdos-Renyi (ER) networks the behavior depends on the routing protocol, when shortest path are applied, the capability decreases, however when random paths are followed the capability increases. We also focus on the relationship between topological robustness and dynamical robustness, by comparing when the network will be first physically split or dynamically collapsed.

The paper is organized as follows. In section 2 we describe the experiments performed. In section 3 we discuss the results obtained. Finally, in section 4 we expose the conclusions of the work and possible future research lines.

2. DESCRIPTION OF THE EXPERIMENT

Here we define the two aspects of the problem we will analyze in this work: the process of node removal and its topological effect, and the change in the onset of congestion for the traffic dynamics when the removal of nodes is performed.

2.1 Topological robustness

A random breakdown of a network can be modeled as a percolation process. The percolation threshold p_c in lattices is defined as the fraction of lattice points that must be filled to create a continuous path of nearest neighbors from one side to another, or equivalently destroyed to ensure that no such a path exists. In complex networks, the percolation threshold is usually characterized by the existence of a giant component with the same diameter as the original network.[1,6] The diameter keeps constant while the size of the giant component is $\sim O(S)$, being S the original size of the network.

In this paper we use a more restrictive approach to determine the percolation threshold akin to that used in lattices. Instead of considering the size of the giant component, we will look for the critical fraction of node removals that avoids the existence of a physical path connecting every pair of the remaining nodes of the network.

The topological robustness of a network is defined then as the probability of maintaining all nodes connected when increasing the fraction p of removed nodes. For $p < p_c$, the probability of having more than one component is zero. For $p > p_c$ the probability shows a transition determined by the statistical properties of the network. We have studied this robustness on three different types of networks: regular lattices, ER and scale-free. For comparison purposes, the three types of networks will have the same number of nodes $S = 1000$ and a similar number of links $L \sim 4000$.

The first type of networks have been implemented as periodical two-dimensional regular lattices with all nodes having the same degree $k = 8$. This type of networks have a very high clustering coefficient and a high mean average path length. The random networks have been created using the Erdos-Renyi model[15] with an edge probability $p = 0.008$. In this case, the networks display a Poisson degree distribution with a mean value of $< k > = 8$, a very low clustering coefficient and also a low average path length. Finally, the scale-free networks have been created using the preferential attachment mechanism of Barabási-Albert (BA)[16] where each node adds $m = 4$ new links, obtaining power-law degree distribution $P(k) \sim k^\gamma$ with $\gamma \sim 3$.

To calculate the topological robustness defined above, we have performed a sequential random degradation process, removing sequentially nodes (and their connections) until the network splits. We have repeated the breakdown 10^6 times to obtain a significant statistical approach.

Fig.2.1 shows the probability of splitting the network (topological robustness) when a fraction of nodes p have been removed. The results are similar to the fragmentation processes exposed in previous articles[1,4]. The probability threshold is lower when the network has a power-law distribution due to the existence of hubs that act as cohesive elements, hardly destroyed by a random process. As a consequence, the network remains connected for larger values of p compared to ER networks. The reason for the robustness of regular networks is different, the high robustness exhibited is a consequence of their high clustering coefficient which provides a high degree of redundancy. In the inset we plot the relative average path length as a function of the number of removed nodes, as expected the average path lengths remain almost constant in all networks, with a slight increment in the ER
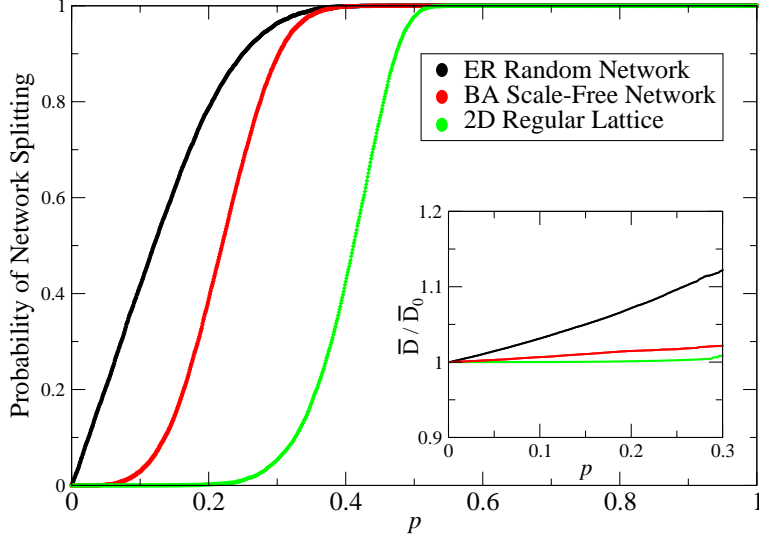
Figure 1. Probability of network splitting in two or more connected components as a function of the fraction of removed nodes p. Inset, relative average path length as a function of p.

networks case. These results in ER and BA networks are in agreement with results of random percolation in complex networks,[1,2,4] showing however a shift in the transition point due to a more restrictive definition of robustness used here.

2.2 Dynamical robustness

In analogy of the topological robustness, the dynamical robustness is defined as the probability of a network to maintain the communication processes between every pair of nodes nodes. When the network splits into two or more components, the communication is also interrupted because the packets are unable to reach the isolated nodes. However, there are some cases where the network is still physically connected but the overlay dynamics is unable to deliver information to certain nodes, provoking some sort of dynamical split of the network. As we have introduced before, the cause of this phenomenon is the emergence of congestion. When a system is congested, a large number of packets get stuck in nodes and never reach their destination.

To study the congestion point we define a set of rules that will drive the evolution of traffic. First, to model the receiving and limited transmission of information of each node, we assign a queue to each one and a different from zero service time. The capability of the nodes of is characterized then by the time needed to serve one packet. We assume this time to follow an exponential distribution with mean $1/\mu$. If a packet arrives when the node is busy delivering another one, it gets stored in a FIFO (first in -first out) queue until it gets dispatched. To simplify the experiments, we will use during the rest of the work a value of $\mu = 1$.

Once we have mapped the queues into the nodes, we introduce the dynamical rules: The packets are created in each node following a Poisson distribution with mean ρ, and they are assigned with a random destination. These packets travel through the network using a static routing protocol (the decision rules are set at the beginning of the experiment). Once the packet arrives at its destination, it is removed from the system.

Since congestion emerges when the incoming traffic to a node is higher than its capability to dispatch it, and we have fixed the value of this capability by the service time, the onset of congestion remains as a function of ρ. The network achieves its steady state when for a certain value of ρ the number of packets of the system at time t, $N(t)$, fluctuates around an stationary value. When the value of ρ overcomes a critical value ρ_c, the number of packets $N(t)$ diverges and the system enters in a congestion phase. Moreover, it has been proved[12] that the onset of congestion is driven by the node with the highest algorithmic betweenness B^*. The algorithmic betweenness of a node B_i is the number of paths that go through node i given a certain routing algorithm. When the incoming traffic that arrives to this node is higher than its delivery capability, $\rho B^*/(S-1) > \mu$, its

queue starts to grow and induces congestion in the network. Therefore, the congestion point of the system ρ_c is determined by the moment at which the node with maximum algorithmic betweenness receives and delivers the same ratio of packets:

$$\rho_c = \frac{\mu(S-1)}{B^*} \tag{1}$$

2.3 Experiments

Our experiments consist then in to analyze the variation of the onset of congestion determined by ρ_c when the system experiments random failures, simulated as the sequential random elimination of nodes, for those networks that after the random failure still remain connected. For each network, we perform a step of the sequential removal of nodes, if the removal of the node does not produces a split on the network we calculate its new ρ_c.

To determine numerically the value of ρ_c for a given configuration we simulate the traffic dynamics. Starting from a value of ρ that provides a steady state, we gradually increase this value and determine whether or not the number of packets floating on the system diverges. The difficulty of deciding if the system is or not at the critical point, increases as ρ approaches ρ_c. To characterize the transition we used an order parameter η[17] :

$$\eta = \frac{N(t+\tau) - N(t)}{\rho\tau} \tag{2}$$

where τ is the observation time. When $\rho < \rho_c$ the order parameter is zero (There is no difference between the ratio of created packets and the ratio of removed). On the contrary, if $\rho > \rho_c$, the value of $N(t)$ grows linearly with t, and the order parameter is a function of ρ[17] .

Before removing nodes, we determine the maximum load that the complete network can handle $\rho_c(0)$. Then we remove a fraction of nodes p and recalculate the maximum congestion value $\rho_c(p)$, repeating this process while the network has more than one connected component. We perform 10^4 simulations of each experiment to obtain an statistical approach of $\rho_c(p)$.

3. ANALYSIS AND DISCUSSION OF RESULTS

In a first experiment we have analyzed the effects of the random breakdown on congestion, when the communication dynamics are based on a shortest path (SP) routing protocol. The results obtained are shown in Fig. 2 (a). We observe different behaviors depending on the topology used: The maximum load in a scale-free network increases with the number of removed nodes, whereas in ER random networks decreases slowly with p.

To understand the results we have studied the changes on the betweenness distribution of both network structures when a node is removed. It has been proved that there is a correlation between the degree and the betweenness distribution in random graphs and in scale-free networks.[6, 18] Since the probability of deleting the node with the highest degree is very small,[1] we can consider as a first approximation that the node with B^* is the same during all the breakdown process.

Another important feature that we can extract from the betweenness distribution is the importance of one node in the communication processes.[19, 20] We characterized the importance of the most important node using α^*, defined as the maximum algorithmic betweenness normalized, $\alpha^* = B^*/\sum B_i$. We can see in Table. 3 that the importance of the most connected node α^* differs significantly in the random and scale-free networks due to their different degree distributions: In the scale-free, 7% of the packets travel through the most central node in contrast with the the 0,52% of the random network.

Every time we remove a node i, we also remove the load it generates L_i,[13] decreasing the value of the B^* according to the importance of this node in the communication process. The load generated by one node is defined as

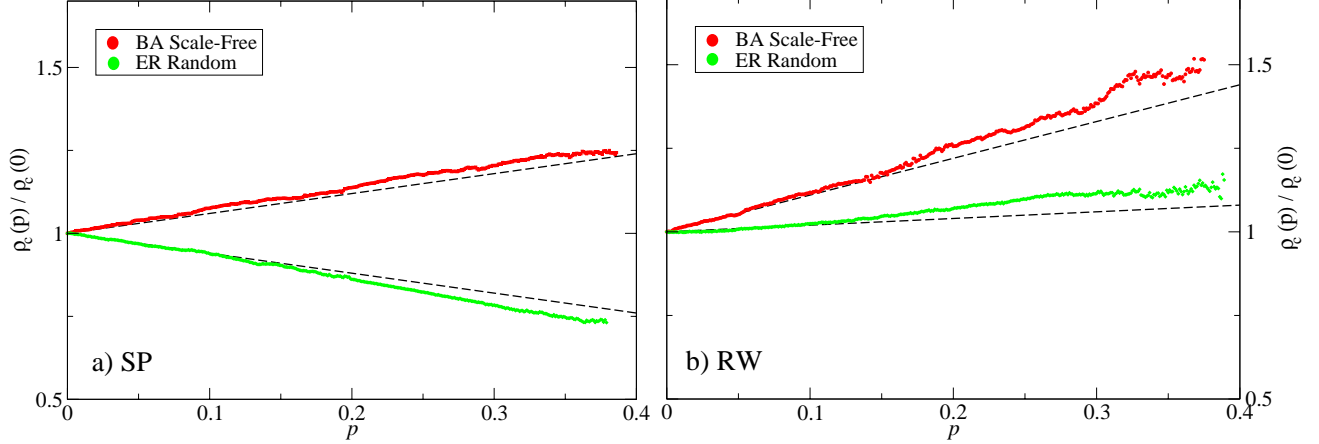$$L_i = \sum_i (D_{i,j} + 1) = (\bar{D}_i + 1)(S-1) \tag{3}$$

Figure 2. Effects of the node removal on the normalized maximum capacity of scale-free and random networks when using a (a) routing protocol based in shortest paths and (b) routing protocol based in random walks. Dotted lines present the analytical approach using Eq. (5) and experimental data from table 3.

where $\bar{D}_i$ is the average path length between node i and the rest of nodes in the network $(S-1)$ (being S the original number of nodes of the network). In a SP routing protocol, this distance measures the average shortest path length from node i to the rest of the network, which can be easily determined using a Dijkstra algorithm[21] . Using eq. (1) we express the onset of congestion for a certain fraction of removed nodes $\rho_c(p)$ for large S as:

$$\rho_c(p) = \frac{(S-1)-pS}{B_{ini}^* - \alpha^* \bar{L}(p)} \sim \frac{S(1-p)}{B_{ini}^*(1 - \frac{\alpha^* \bar{L}(p)}{B_{ini}^*})} \tag{4}$$

where pS is the number of removed nodes and $\bar{L}(p)$ is the amount of load that we have withdrawn of the network after deleting pS nodes, which can be approximated by $\bar{L}(p) \sim pS\bar{L}$, where $\bar{L} = \frac{1}{N}\sum_i L_i$. Eq. 4 can be approximated using a Taylor expansion, obtaining

$$\rho_c(p) \sim \frac{S}{B_{ini}^*} + p\frac{S}{B_{ini}^*}\left(\frac{S\bar{L}\alpha^*}{B_{ini}^*} - 1\right) + O\left[\left(\frac{pS\bar{L}\alpha^*}{B_{ini}^*}\right)^2\right] \tag{5}$$

Considering that $pS\bar{L}\alpha^*/B_{ini}^* << 1$ when $p << 1$, using Eq. 5 we can determine the expected initial behavior of the congestion point analytically. When $S\bar{L}\alpha^*/B^* > 1$ the maximum load supported by the system starts to grow as the node suffers a random removal, and the initial slope of the congestion is $S\bar{L}\alpha^*/B^* - 1$. Otherwise, if $S\bar{L}\alpha^*/B^* < 1$ the maximum load decreases with the node removal. Introducing the values presented in Table 3 in eq. 5, we have represented in Fig.2 the expected behavior of $\rho_c(p)/\rho_c^{ini}$, obtaining a good agreement with the computational simulations.

Network	Protocol	B_{ini}^*	α^*	D	L	$S\bar{L}\alpha^*/B^* - 1$
BA Scale-free	Shortest Path	$1.5*10^5$	0.07	3.3	3300	0.54
ER Random	Shortest Path	$1.3*10^4$	0.0052	3.8	3800	-0.52
BA Scale-free	Random Walk	$2.2*10^7$	0.029	1595	$1.6*10^6$	1.1
ER Random	Random Walk	$2.9*10^6$	0.0024	1380	$1.4*10^6$	0.15

Table 1. Values of the maximum algoritmic betweenness B^*, the importance of this betweenness in the communication process α^*, the average path length $\bar{D}$, and the average generated load by one node $\bar{L}$ for the scale-free and random networks using SP and RW routing protocols. The value of $S\bar{L}\alpha^*/B^* - 1$ determines the change of the congestion point when removing a fraction of nodes p.

We have also analyzed the ratio $\rho_c(p)/\rho_c(0)$ when packets are delivered using a random walk (RW) routing protocol.[22] The RW betweenness distribution for a random walk process has been studied by Newman,[23] showing that it shares the properties of the SP betweenness. Table 1 shows that when we use a RW routing protocol the statistical values increase significantly. The average path length of a packet to reach its destination is much higher than the shortest path, since the packets do not have information about how to reach their destination. This distance can be determined analytically using the mean first-passage time between two nodes.[22] Since the distance is much higher, the amount of load introduced by the nodes is also higher, and therefore the value of B^* increases. The results obtained (see Fig. 2(b)) show that using a RW routing protocol, the initial congestion behavior is also governed by the evolution of the B^* described in Eq. 5, although a larger deviation is observed for larger values of p in agreement with the discussion above.

We have performed a second experiment to investigate the behavior of the congestion when the underlying topology is a regular lattice, see Fig. 3. This type of network is interesting because the changes on the congestion can not be described in the previous approximation. The explanation for the behavior observed in Fig. 3 is the
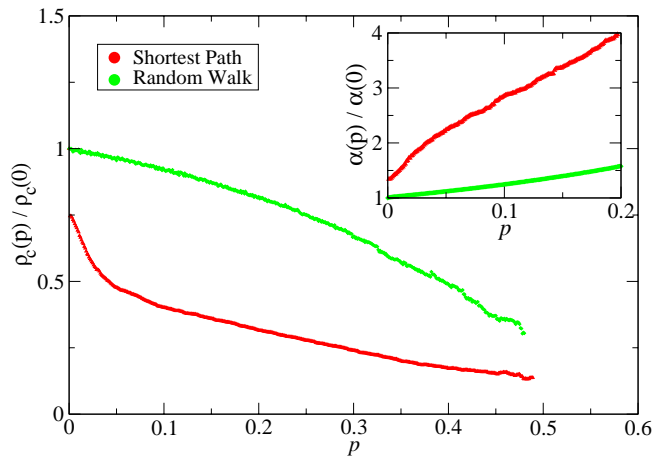

Figure 3. Effects of the node removal on the normalized maximum capacity of a 2D regular lattice networks when using a routing protocol based in shortest paths and random walks. In the inset we plot the evolution of the relative importance of the node with maximum betweenness as a function of p.

following. Before removing any node of the regular network, all of them have the same algorithmic betweenness because the underlying symmetry. When a little fraction of nodes has been removed, the shape of the betweenness distribution changes, and some nodes become relevant in the communication process. The changes of this centrality are characterized by the changes of α^*. In the precedent analysis we have considered that the value of α^* is constant because the failures does not modify significantly the structural properties. However, in the regular network this process change the structure breaking symmetry, and the value of α^* becomes now a function of the number of removed nodes. The inset of Fig. 3 shows the evolution of this parameter when we remove a certain fraction of nodes. Since the value of the maximum betweenness is a function of α^*, when this value grows B^* also grows and the onset of congestion decreases.

3.1 Topological robustness vs dynamical robustness

As we have introduced so far, when a network suffers random failures there exists the possibility that some nodes of the network get isolated from the communication process. The causes of this isolation can be topological, if the network splits, or dynamical, when congestion emerges and avoids the proper distribution of information. To discover which one of this two causes will appear first given a certain topology and routing protocol, we have compared the probability of disconnecting the network physically versus the maximum congestion of the network, when removing a fraction p of nodes. We use again the three network topologies and the two routing protocols presented before, obtaining the results presented in Fig. 4.
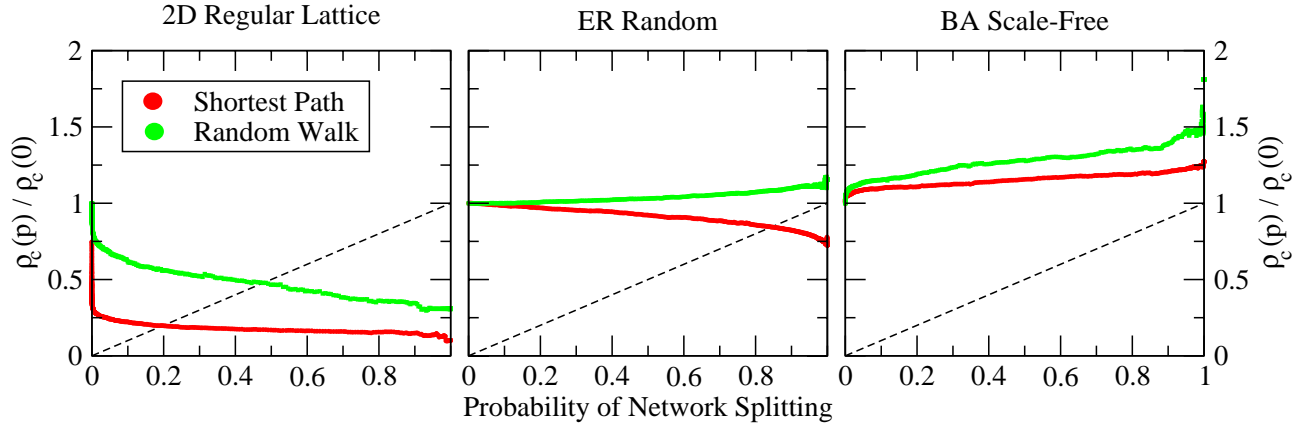
Figure 4. Dynamical robustness versus topological robustness. The dashed line delimits the probability of splitting the network. The crossing between the relative congestion ratio $\rho_c(p)/\rho_c(0)$ and the dashed line determine the change of the dominant effect between both processes. Before this point splitting dominates, beyond this point congestion dominates the communication process after random failures.

This comparison provides some insights about the robustness of the communication process, defining regions of the parameters for which congestion is attained before splitting the network and vice versa. First we find that SF networks show a very high dynamically robustness. This means that, even if the system is functioning at his maximal capacity before removing any nodes, the random failures will not introduce congestion into this system. In second place, we find that regular networks are more topologically robust. If the communication process is based on a RW routing protocol and the initial system works at the 50% of the maximum capacity, a random breakdown will introduce congestion in the network before splitting into two components. If the routing protocol is based in SP, the maximum capacity to avoid the congestion decreases to the 20% of the total. With higher values of the initial load, the system will fail dynamically before topologically.

Finally, the robustness of random networks depends on the routing protocol. Using a SP, the communication process can operate up to the 80% of its capacity avoiding congestion. If we change the protocol to RW, we observe that the network improves its dynamical robustness, being very difficult to congest it via random failures.

4. CONCLUSIONS

In summary, in this work we have studied the relationship between the random breakdown of a complex network and the congestion point of communication processes. We have proved that this relationship is governed by the algorithmic betweenness distribution. Moreover, we found that the centrality of the most important node in the communication process (the node with the highest betweenness) plays a crucial role in the changes of the onset of congestion. We presented an analytical expression for the behavior of the onset on congestion which is based on the amount of traffic that we remove from the node with maximum algorithmic betweenness, confirming its validity using different topologies and routing protocols. We also observed that if the breakdown modifies structural properties, the centrality of the nodes also changes, obtaining a different behavior of the congestion point.

The results provide some insight of the dynamical response of a network when there occur random failures. In other words, they give us an idea of the load a system can handle if we want to avoid the congestion, in case the network suffers random failures. These results play an important role when modeling communication process in real networks. For instance, they can be used in the design of a dynamic communication process to guarantee the efficiency when some of the nodes have been removed.

Some interesting issues remain open for future studies. We expect that changing the topology or the routing protocols we will be able to observe different slopes for $\rho_c(p)/\rho_c(0)$ governed by the same constrains exposed in the work. Another appealing work derived from this problem is the analysis of the the congestion when the network undergoes an intentional attack.

REFERENCES

1. R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature* **406**, pp. 378–382, 2000.
2. R. Cohen, D. ben Avraham, and S. Havlin, "Percolation critical exponents in scale-free networks," *Phys. Rev. E* **66**, p. 036113, 2002.
3. L. Gallos, R. Cohen, P. Argyrakis, A. Bunde, and S. Havlin, "Stability and topology of scale-free networks under attack and defense strategies," *Phys. Rev. Lett.* **94**, p. 188701, 2005.
4. R. Cohen, K. Erez, D. ben Avraham, and S. Havlin, "Resilience of the internet to random breakdown," *Phys. Rev. Lett.* **85**, pp. 4626–4629, 2000.
5. R. Cohen, K. Erez, D. ben Avraham, and S. Havlin, "Breakdown of the internet under intentional attack," *Phys. Rev. Lett.* **86**, pp. 3682–3685, 2001.
6. P. Holme, B. Kim, C. Yoon, and S. Han, "Attack vulnerability of complex networks," *Phys. Rev. E* **65**, p. 056109, 2002.
7. D. Callaway, M. Newman, S. Strogatz, and D. Watts, "Network robustness and fragility: percolation on random networks," *Phys. Rev. Lett.* **85**, pp. 5468–5471, 2000.
8. B. Tadic, G. Rodgers, and S. Thurner, "Transport on complex networks: Flow, jamming and optimization," *International Journal of Bifurcation and Chaos* **17**(7), 2007.
9. V. Latora and M. Marchiori, "Efficient Behavior of Small-World Networks," *Physical Review Letters* **87**, p. 198701, Nov. 2001.
10. P. Crucitti, V. Latora, M. Marchiori, and A. Rapisarda, "Efficiency of scale-free networks: error and attack tolerance," *Physica A* **320**, pp. 622–642, 2003.
11. E. Lopez, R. Parshani, R. Cohen, S. Carmi, and S. Havlin, "Limited path percolation in complex networks," *cond-mat* **070269**, 2007.
12. R. Guimerà, A. Díaz-Guilera, F. Vega-Redondo, A. Cabrales, and A. Arenas, "Optimal network topologies for local search with congestion," *Phys. Rev. Lett.* **89**, p. 258701, 2002.
13. A. Motter, "Cascade control and defense in complex networks," *Phys. Rev. Lett.* **93**, p. 098701, 2004.
14. P. Crucitti, V.Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Phys. Rev. E* **69**, p. 045104, 2004.
15. P. Erdos and E. Renyi, "On the evolution of random graphs," *Publications of the Mathematical Institue of the Hungarian Academy of Sciences* **5**, pp. 17–61, 1960.
16. A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science* **286**, pp. 509–512, 1999.
17. A.Arenas, A. Díaz-Guilera, and R. Guimerà, "Communication in networks with hierarchical branching," *Phys. Rev. Lett.* **86**, pp. 3196–3199, 2001.
18. K. Goh, B. Kahng, and D. K. D, "Universal behavior of load distribution in scale-free networks," *Phys Rev Lett.* **87**, p. 278701, 2001.
19. M. Barthelemy, "Betweenness centrality in large complex networks," *Eur. Phys. Jour. B* **38**, p. 163, 2004.
20. V. Latora and M. Marchiori, "A measure of centrality based on the network efficiency," *cond-mat/0402050* , 2004.
21. T. Cormen, C. Leiserson, R. Rivest, and C. Stein, *Introduction to Algorithms, Second Edition*, MIT Press and McGraw-Hill, 1990.
22. J. Noh and H. Rieger, "Random walks on complex networks," *Phys. Rev. Lett.* **92**(11), p. 118701, 2004.
23. M. Newman, "A measure of betweenness centrality based on random walks," *Social Networks* **27**, pp. 39–54, 2003.