A self-repairing solution for the resilience of networks to attacks and failures

Nicolas Brax*, Frédéric Amblard^

* CNRS-IRIT, 118 route de Narbonne, 31062 Toulouse

^Université de Toulouse 1 Sciences Sociales – 2, rue du doyen Gabriel Marty, 31 062 Toulouse Cedex 9

frederic.amblard@univ-tlse1.fr

Abstract: Robustness against failures and attacks is an important characteristic for real networks. Although methods have been proposed making networks more resistant, they are often designed to rehash networks before issues occur. In this paper, we investigate three dynamic methods making the network being able to repair itself while under massive attacks and failures. We consider two different topologies, Erdos – Renyi random graphs and Barabasi – Albert scale-free networks, and find out that a local strategy is able to maintain, at least for a moment, the network relatively connected. We believe this rewiring algorithm interesting because it might be not very difficult to implant in real networks and it provides a dynamic response while other arrangements are taken to answer the threat or the issues.

Keywords:large connected component, random graphs, robustness, scale-free networks, self-repairing networks, structure of complex networks

1.Introduction

The point of view on complex systems as networked structures of interacting elements is wide spreading. Analysing very different corpus in different disciplines (biology, computer sciences, traffic and so on...) some shared properties have been identified (scale-free structure for instance) on static structures. The modelling of the formation of such structures is still a key-point, even if some proposal exist (preferential attachment dynamics by Barabasi and Albert) as well as many works concerning dynamics occuring on networks (for instance information spread or opinion dynamics or cooperation dilemma). Among those latter works, Barabasi and Albert (2001) proposed to study the impacts of failures and attacks on scale-free networks. Their main finding was that concerning random failures, scale-free networks are much more robust than random ones and that concerning intentional attacks, random networks are much more robust than scale-free networks. However, not much works exist concerning possible robust solutions in order to repair networks after an attack or a failure and their consequences on the structure of the underlying network itself. In this paper, we propose to study three simple strategies for the reparation of networks after an attack or a failure ; to study the efficiency of those solutions applied either on random or on scale-free networks and to study the impacts of those strategies on the structure it is applied on, as when applying a repairing strategy you necessarily modify the network and potentially its macroscopic properties. Section 2 will give an overview of related works in the field. Section 3 presents the models we use and section 4 presents the results we obtained from simulations. The final section discussed the overall approach and proposes some further steps to our research.

2.Related works

Numerous systems in the real world can be represented as networks where nodes are the components and edges symbolize an interaction between two components. Analysing those networks a shared property that is often identified is the scale-free property of the distribution of links per nodes. Some examples are the World Wide Web (Barabasi &al. - 1999), citation networks (Redner – 1998), cellular (Jeong et al. - 2000) or protein networks (Scala, Amaral & Barthelemy – 2001). In order to understand mechanisms that produce such structures, various models have been proposed so far. The first of them is probably the random-graph model of Erdos-Renyi (Erdos & Renyi – 1959). This model defines a random graph as *N* nodes connected by *n* edges randomly chosen from the *N(N-1)/2* possible ones. In this paper, we used the alternative binomial model, starting with N nodes and every pair of nodes connected with a probability *p*. Such graphs have some significant properties like the degree distribution following a Poisson law (Erdos & Renyi – 1959 ; Bollobas – 1985), the low diameter compared to the one of equivalent regular graphs (Chung and Lu – 2001), efficiency (Latora and Marchiori – 2001) or the low clustering coefficient compared to either random or small world networks (Watts and Strogatz – 1998). Moreover, they give an opportunity to set up a comparison with real networks (Newman – 2001).

Since Barabasi and Albert (1999), it is known that many real networks degree distribution follows a power-law and that random graphs are not able to render either the scale-free or the small world characteristics of those real networks. Another model ensuring a short path length and a relatively high clustering coefficient is the Watts-Strogatz small world model (Watts and Strogatz – 1998). But this model cannot reproduce the power-law degree distribution of many real networks. To render this, Barabasi and Albert (1999) have proposed two generic mechanisms responsible of the scale-free networks emergence : growth and preferential attachment, giving a new vision of the network study.

Network analysis is a wide field of investigation. As they offer dynamical processes, they can be useful to determine and understand some dynamical features in the real world. Within this field, the robustness of networks against attacks and failures is one of interest for us in this paper. Networks like the Internet are often disturbed by router failures (Barabasi - 2002), and we can imagine that major troubles could occur if you put down the central points of the Internet or of a telecommunication network. Therefore it is important to propose efficient repairing strategies. The major use of such solutions is in computer science with networks such as peer-to-peer networks or, globally, the Internet. But we can also envisage some suitable solutions for telecommunication networks. Indeed, theses networks can undergo some accidental failures (local cut, overload, ...) or natural local issues (storms, earthquakes, ...) that we can take into account in our model as random failures.

It is known that scale-free networks are robust against failures but highly vulnerable against attacks, i.e. when the hubs are preferentially targeted (Barabasi - 2000). On the other hand, it has been shown that random networks have a similar tolerance to failures and attacks. Furthermore, we can say that the robustness of a network to failures and attacks depends on its topology (Crucitti and al. - 2004).

To avoid those troubles, responses have been envisaged, mainly the modification of the network topologies to improve network robustness (Beygelzimer and al. - 2005 ; Moreira and al. - 2008). The idea is to prevent attacks damages by modifying the edges. However, in real networks, you cannot always rehash a network before an attack or a failure occurs. This happens in most of the real telecommunication networks where algorithms are settled up to prevent failures or to compensate the loss (Kuhn and al. - 2005). Csardi and al. (2004) have proposed a solution where the network reacts immediately after the disappearance of a node. On random networks, their second neighbours rewiring strategy seems to be a good solution, allowing the network to grow again, even facing numerous severe attacks (a result that we have not been able to reproduce). In our paper, we examine results on both random graphs and scale-free networks.

3. Models description

We first describe the models we used for the underlying graphs and in the next section the model we used to simulate failures and attacks on these graphs.

a) Graph Models

For some simplicity reasons and aiming at comparing our results with existing approaches, we only considered undirected and not weighed networks in this paper. We used two different graph models. First, we used the Erdös-Rényi random graph model (Erdos and Renyi, 1959), constructed from an initial set of N unconnected nodes and adding K edges between pairs of randomly chosen nodes, avoiding the repetition of links and self-loops in the network. If the sparseness condition is verified, i.e. $K <= N2$, the model provides a Poisson distribution of nodes' degrees. Second, we used scale-free networks, built using the Barabasi-Albert preferential attachment model (Barabasi and Albert, 1999). In this latter, we first draw an initial set of fully-connected nodes and then we iteratively add a new node at each iteration and connect it to the existing network using preferential attachment, i.e. the probability for the new node to be linked to an existing node depends linearly on the number of links of this node. According to Barabasi and Albert, this model results in a graph exhibiting a power-law distribution of nodes' degrees.

b) Failure and Attack

In this paper, we study the efficiency of rewiring strategies after failures and/or attacks on those two different types of networks. By failures, we mean the random suppression of a node in the network. It renders real phenomena like accident/shut-down on a telecommunication or a P2P network. On the other hand an attack corresponds to the removal of a node having a higher degree, representing, for instance, an intentional attack over a network where the attacker (hacker) wants to make as much damage as possible. Some stochastic heuristics enable to easily find such nodes without having to know the whole structure of the network. In this paper we adapted the heuristics proposed by (Cohen & al., 2003), i.e. in order to attack nodes with a higher degree, the attacker chooses first a random node from the whole network, and then a random neighbour of this node. As the final attacked node has a probability kp_k of having a degree k, where p_k stands for the degree distribution of the network. It results in a more probable attack of node having a higher degree.

c) Rewiring strategies

When an attack occurs, the neighbours (we call them the ***affected*** nodes) of the ***attacked*** node (cf. Fig.1a) act as so to try and keep the whole network connected. Here, we consider three possible strategies: A) the random rewiring (cf. Fig.1b) where affected nodes randomly connect to other nodes in the network; B) the greedy rewiring strategy (cf. Fig.1c) where affected nodes try to connect to a high degree neighbour of a random neighbour; C) the second neighbour strategy (cf. Fig. 1d), proposed by Csardi and al. (2004) where affected nodes attempt to connect themselves. Intuitively, we can say that the first strategy will keep the random graph unchanged while a scale-free network will have the tendency to become a random graph quite rapidly. For the second strategy, we can easily say that it won't avoid the breaking of a random graph, even less for a scale-free network because there is no way to reconnect separate parts of the graph. The third strategy tries to conserve the structure of the network by connecting affected nodes among each others.

To study the resulting topology of a network after a massive amount of attacks or failures and using one of the rewiring strategies, we keep the number of nodes constant. So as soon as there is a deleted node in the network, we add a new one to it. The connection of the new node to the rest of the network depends on the tested structure. As for a random graph the new node will get connected to a randomly chosen one, in a scale-free network the new node will connect to a node with higher degree. Such a solution will avoid the graph to collapse after some attacks because all nodes were deleted.

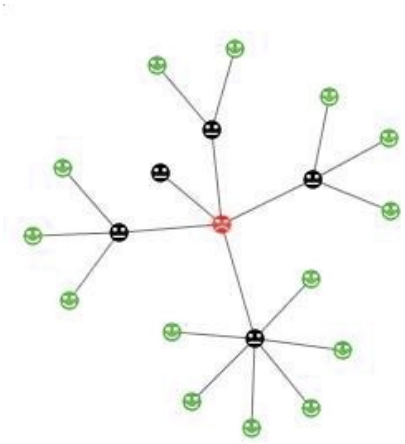

Figure 1a: The attacked node is the red one, the affected nodes are the black ones

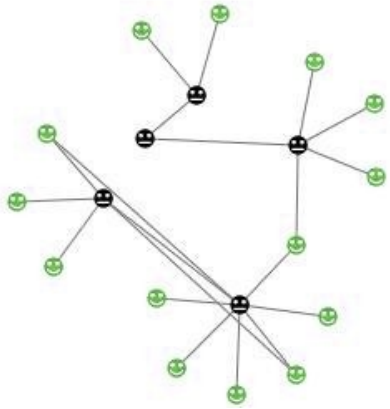

Figure 1b: Random rewiring (A) of the affected nodes with random nodes of the network

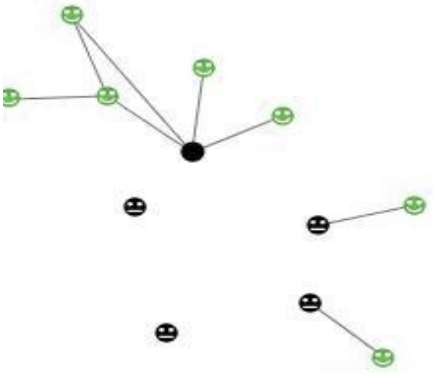

Figure 1c: Greedy rewiring (B) of affected nodes with a good neighbour of a random neighbour

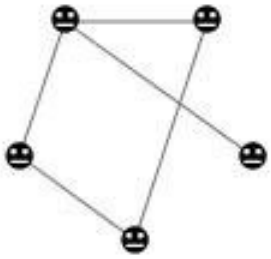

Figure 1d: 2nd neighbour strategy (C), affected nodes rewire each others

d) Indicators used

There is a lot of valuable properties like average or characteristic path length, diameter, clustering coefficient and others, each one allowing to study some particular characteristics of the network (Newman and al. - 2006). We have chosen to consider the size of the largest connected component. This is quite a basic indicator but it renders quite well the idea of how healthy or robust the network is either to failures or attacks. Due to the construction methods, the initial size of the component can be N in case of a scale-free network and about 0.9N in case of a random one. This is because in a scale-free network, each new node will connect to the existing network so no node can be isolated. Whereas in a random graph, we chose pair of nodes to build the graph and there is a probability to leave some nodes alone but it is assumed that there is a phase transition in random graph with increasing the edge density at which a giant component forms. For a large enough degree, this component fills a large portion of the graph while all other components are relatively small.

4. Results

In this section we will present each one of the strategies considered, i.e. A) random rewiring, B) greedy rewiring and C) second-neighbour strategy, testing for each strategy the random and scale-free structures. In each case, we will observe the consequences of both failure and attack scenarios.

A) random rewiring

The first strategy (A) is the most simple one: affected nodes rewire to a randomly chosen node of the network. In a real network, it is usually not relevant as it would imply that each node of the network would know the entire network in order to choose a newer node to get linked to. The basic aim of this hypothesis is rather to take a null hypothesis for comparison with more reasonable assumptions. More concretely, we will check in the simulations whether or not the network structure remains stable or if it is perturbed and how. We will also observe whether or not the network still exhibits a giant component along the attacks and we will measure the evolution of its size.

A.1) random graphs

A.1.a) Natural failure

In this case, as the deletion of nodes and the rewiring of links follow random processes, there is no collapse of the network and the size of the giant component remains constant along the simulation. Moreover, if the initial graph includes some isolated nodes, these latter can be chosen with a probability 1/N by the affected nodes as targets along the rewiring process, enabling them to become apart of the giant component. This explains why the ratio of the giant component grows to 1 on the figure 2, meaning that all nodes are apart of the network.

A.1.b) Targeted attack

The attack process has the same consequences than the failure process we just described and the figure 3 shows a similar plot than on figure 2. Even if the removed nodes are preferentially the ones with a higher degree (higher degree being targeted by the attacks), the random structure ensures, at least in the beginning, quite an egalitarian distribution of the links in the network, i.e. all nodes have nearly the same degree. The random rewiring does not change the global distribution of links in the network, even under attacks. And therefore, the initial random graph remains random to this respect. To say it simple, it is only because nodes are approximately equals in terms of degree that attacks are not much efficient than failures on this topology, this conclusion was risen yet by Barabasi and Albert (2001). However, we have to mention that the characteristic distribution of random network (i.e. Poisson law) is slightly deformed, deleting the right part of the curve (those nodes being preferentially targeted by the attacks). It follows that the bell curve moved slightly to lower degrees. In this respect, if the random rewiring conserves the qualitative aspect of an egalitarian distribution, it does not conserve the characteristic distribution of a random network.

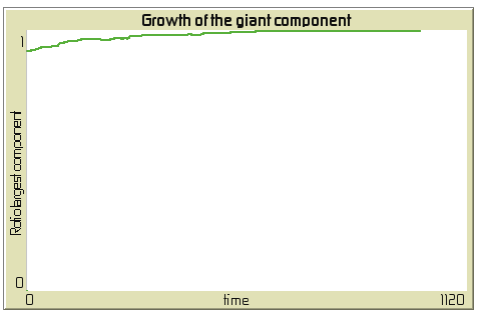

Figure 2: Random rewiring of random graph after failure

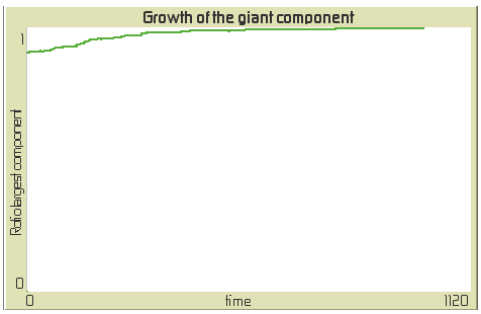

Figure 3: Random rewiring of random graph after attack

A.2) scale-free networks (Fred : Arrêté là)

A.2.a) random failure

Barabasi and Albert (2002) demonstrated the robustness of scale-free networks to random failures and their higher sensitivity to targeted attacks when compared to random networks. From our experiments, we observed the same robustness feature to random failures when adding random rewiring (see Figure 4). Moreover, concerning the degree distribution, starting with a power-law one, the addition of random rewiring tends to give the networks some random graph characteristics (i.e. the power-law tends to be transformed step by step into a bell curve that is characteristic of a Poisson law).

A.2.b) targeted attack

According to our experiments, a random rewiring strategy enables to keep the giant component's size quite constant, as shown on figure 5. However, and just as for random failures, the power-law distribution tends to disappear to the favour of a distribution that corresponds more to a random network. It could be interesting to study more precisely how the structure evolves and to see how it impacts others indicators, we do not detail this point in this paper.

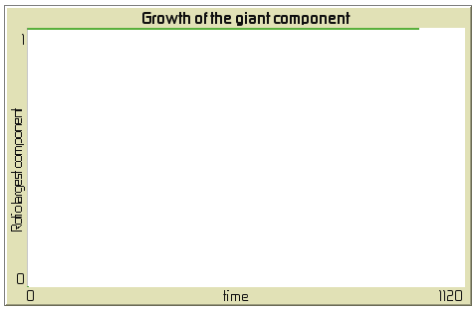

Figure 4: Random rewiring of scale-free network after failure

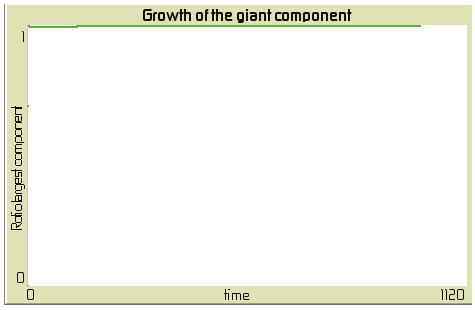

Figure 5: Random rewiring of scale-free network after attack

B) greedy strategy

The preceding random rewiring strategy gives good results, keeping the whole network connected. However, it seems to be a difficult strategy to implement for real network as it implies that each node knows all the other nodes of the network in order to choose another one of them randomly. In this respect a more local strategy would be a more feasible solution.
The so-called greedy strategy (B), that we will present now is a local strategy and therefore a more plausible one to be implemented. The greedy strategy acts simply as follows. Knowing only its immediate neighbourhood, an affected node tends to rewire to a node in this proximate neighbourhood. To do that, let's assume that the affected node chooses one of its random neighbours and then chooses the best neighbour (the one with the highest degree) of this selected neighbour.

B.1) random graphs

B.1.a) random failure

The figure 6 shows that the size of the giant component quickly goes down. On the network, it is the result of the burst of it. It can be easily explained because the greedy strategy is not able to reconnect two separate components. So if a node with a high betweenness is chosen, the network will inevitably split and never reconnect, then this rapidly lowers the size of the largest component. And more, after a certain time, we can see a brutal drop. This is explained by the topology of the

resulting network. As we can't reconnect separate components, after numerous failures, the network is split into several smaller graphs with a quite high clustering coefficient. So there is a higher probability to randomly choose a node with the higher betweenness and then split again a small graph into two part, accentuating again the collapse of the network.

B.1.b) targeted attack

As we can see on figure 7, it is the same as above except that there is a faster drop of the giant component size. This is because a important node of a network is often a node with a high betweenness so the separation of the network into two parts and more appears more rapidly.

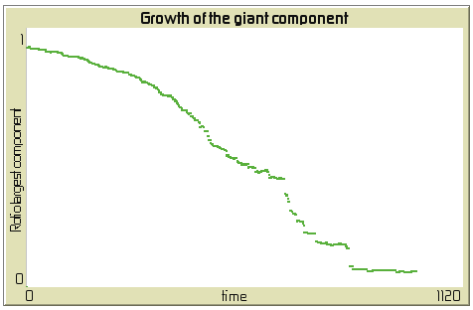

Figure 6: Greedy rewiring of random graph after failure

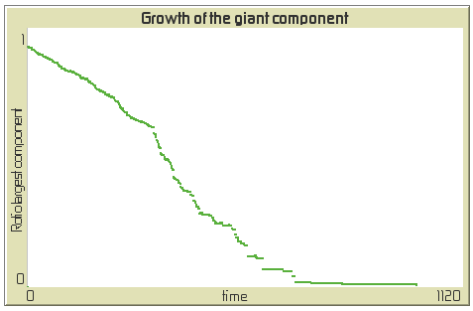

Figure 7: Greedy rewiring of random graph after attack

B.2) scale-free networks

B.2.a) random failure

As for random graph, this strategy on scale-free prevents two different networks to connect themselves so, as soon as there is the suppression of a high betweenness node, the graph splits up. It is quicker than with a random graph because theses nodes are often hubs in scale-free networks and neighbours of a hubs have few connections each others. So in case of the suppression of a hub, with the greedy rewiring, they won't rewire each other and the network will split into several smaller graphs. The figure 8 shows the result as the giant component size falls.

B.2.b) targeted attack

In this case, it is exactly the same explanation as above with a small addition. As we targeted high degree nodes first, the fall of the giant component size is more marked as shows the figure 9 where we can see that, in a few step only, the network is nearly fully disconnected. Then, with time going on, as attacks still occur, the network become composed of only isolated nodes.

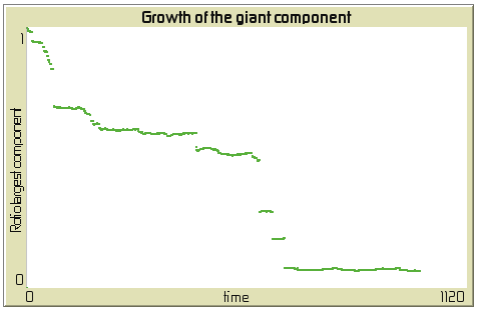

Figure 8: Greedy rewiring of scale-free network after failure

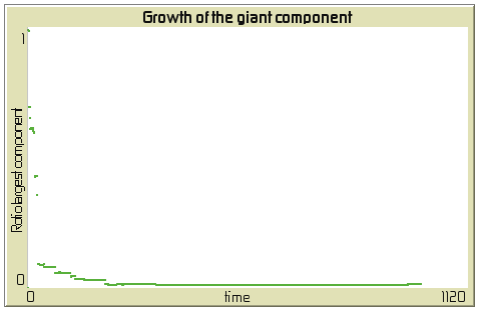

Figure 9: Greedy rewiring of scale-free network after attack

C) second neighbour strategy

We just saw that the greedy strategy can't be a good one if the main goal is to keep the network connected. Indeed, in case of the remove of a node or a link with a high betweenness, there is a high probability to break the network into two parts or more. This probability is even stronger if we consider a scale-free network. To avoid this phenomenon, we investigate the second neighbour strategy (C) which is the rewiring of the affected nodes each others. Again, there is no need of the whole neighbour knowledge but only of the affected nodes, so this imply that nodes keep a list of their neighbours of their neighbours, i.e. their second neighbours, in order to connect with them if a neighbour disappears.

C.1) random graphs

C.1.a) random failure

The figure 10 shows there is a slow decrease of the size of the giant component due to a low separation rate of a little number of nodes, i.e. sometimes there is one or two nodes splitting from the network and never reconnect. On simulation, it is relatively blatant that the topology of the network tends to change from random to scale-free, but further investigations are needed to determine if we really obtains a scale-free distribution or a approaching one, and how it happens.

C.1.b) targeted attack

As for random failure, there is a slow decrease of the largest component size compared to the greedy strategy. However, the decrease is more marked than the one due to a random failure. We can explain it by the topology change of the network. As it tends to gain some scale-free properties, it becomes less resistant to targeted attack (Barabasi – 2000).

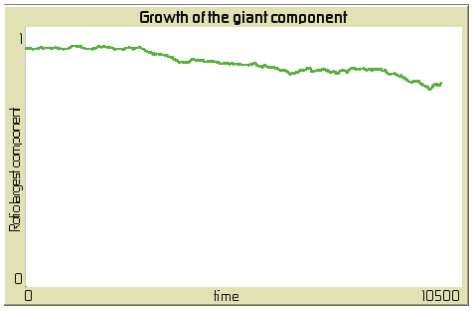

Figure 10: 2nd neighbour rewiring of random graph after failure

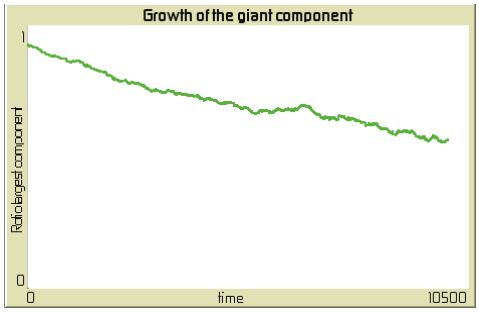

Figure 11: 2nd neighbour rewiring of random graph after attack

C.2) scale-free networks

C.2.a) random failure and targeted attack

We can see on figures 12 and 13 that after a brutal decrease of the largest component size, there is a stabilization of the size for a while and then another brutal drop and stabilization. A scale-free network is not strong versus targeted attack due to the hubs keeping a certain connection within the network so if you put down a hub, you destroy a major part of the network. The second neighbour strategy tries to avoid this by rewiring the affected nodes each others. An other way to say it is that affected nodes try to replace by links the node just removed. To go further, we can say that the hub removed is replaced by a set of nodes, its neighbours, with a relatively high clustering coefficient, and other nodes connected to this set. So it keeps a global scale-free topology with local cluster taking place of hubs. For that, targeting a good node of the network becomes less destructive

than before and give levels where the networks is in a quite stable state because even if you remove a high degree node, we can assume that the others from the "set-hub" keep the connection with others nodes. The brutal decrease appears when the "set-hub" contains one or two nodes, so it is quite the same thing that the initial topology where when you delete an important node, even with the rewiring strategy, you could split important of the network from the largest component. An interesting point is that we have relatively similar plots, both with random failures and targeted attacks. So we can say that even under targeted attacks, the second neighbour strategy is able to keep a relatively large component and not destroying the whole network like the greedy strategy. So, even if it splits the network in some parts and in the very long term the networks collapse, this rewiring algorithm give times to find a response. Furthermore, what we can observe on simulation is that there is not a single large component but several. Indeed, the network splitting globally results in a cut of the largest component in two components of equivalent size. So even if a node is not part of the largest resulting network, it is not isolated for all that.

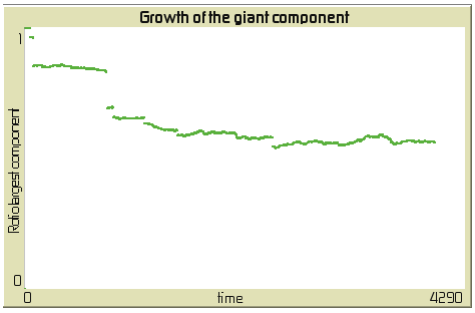

Figure 12: 2nd neighbour rewiring of scale-free network after failure

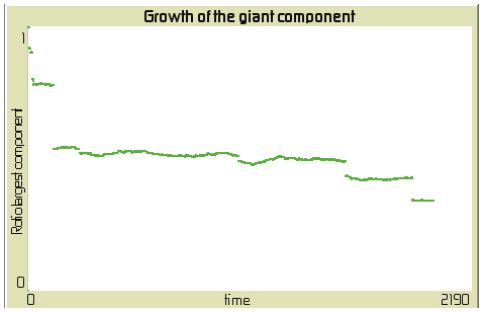

Figure 13: 2nd neighbour rewiring of scale-free network after attack

5. Conclusion

In this paper, we have observed the now known results saying random graphs are relatively robust to both failures and attacks while scale-free networks are highly vulnerable to attacks. Furthermore, we have observed some interesting results when affected networks do not stay passive and react to the suppression of nodes. According to this, we have settled up three strategies : A*) the random* rewiring, B) the greedy rewiring and C*) the second neighbour* rewiring.

First, we have saw the random rewiring giving some good results, keeping the whole network connected. However, we can say it is a unmanageable strategy for real networks because it implies that each node have a full knowledge of all the other nodes in order to randomly choose one of them and connect with it.

Second, we have observed that the greedy rewiring has a major drawback. Indeed, if the suppressed node is the last link between two sub-graphs, the greedy rewiring will not avoid the separation. And if it is destructive against scale-free networks, we have saw that random graphs have not a really better resistance to this. In the end, the network consists in a set of isolated nodes with no links.

Third, we can say that the second neighbour rewiring seems to be a good strategy. As it tries to replace the deleted nodes by links, it gives better results than the greedy strategy, avoiding the full destruction of the network. Furthermore, it is more interesting than random rewiring because it is a relatively local strategy and it tends to keep the initial topology of the affected network, and it seems to leave less isolated nodes. And if scale-free networks fall down, we have observed levels, giving time to take arrangements to counter failures and / or attacks.

It can be interesting to conduct more numerical experiments to find out if the second neighbour strategy is a good one for real networks, meaning networks with a very high number of nodes (hundred of thousands). Also, it is important to take a look to the evolution of the other structural properties of a network, like the path length or the clustering coefficient, allowing to see if the second neighbour algorithm affects these or not, and how, and saying if it is a good rewiring according to the desired characteristics of the initial networks. And, finally, we can assume that nodes are not the only possible target for failures or attacks and defensive strategies are adaptable to link failures and or attacks. An interesting question is if a strategy is effective for both nodes and link suppression or if it gives totally different results.

References

Albert R., H. Jeong H. and Barabasi A.-L., 2000, Nature 406, 378-382, *Error and attack tolerance of complex networks*

Albert R. and Barabasi A.-L., 2002, Review of modern physics 74, 47-97, *Statistical mechanics of complex networks*

Barabasi A.-L. and Albert R., 1999, Science 286, 509, *Emergence of Scaling in Random Networks*

Beygelzimer A., Grinstein G., Linsker R. and Rish I., 2005, Physica A 357:3-4, 593-612, *Improving network robustness by edge modification*

Bollobas B., 1985, Discrete Math. 33, *Random Graphs*

Chung F. and Lu L., 2001, Adv. Appl. Math. 26, 257, *The Diameter of Sparse Random Graphs*

Cohen R., S. Havlin S. and ben Avraham D., 2003, Physical Review Letter 91, *Efficient immunization strategies for computer networks and population*

Crucitti P., Latora V., Marchiori M. and Rapisarda A., 2004, Physica A 340, 388-394, *Error and attack tolerance of complex networks*

Csardi G., Young M., Sager J. and Haga P., 2004, arXiv:cond-mat/0408248v1, *Self-repairing Peer-to-Peer networks*

Erdos P. and Renyi A., 1959, Publicationes Mathematicae, *On the evolution of random graphs*

Girvan M. and Newman M.E.J., 2002, PNAS 99, 7821-7826, *Community structure in social and biological networks*

Jeong H., Tombor B., Albert R., Oltvai Z. N. and Barabasi A.-L., 2000, Nature 407, 651, *The large-scale organization of metabolic networks*

Kuhn F., Schmid S. and Wattenhofer R., 2005, LNCS 3640, 13-23, *A Self-repairing Peer-to-Peer System Resilient to Dynamic Adversarial Churn*

Latora V. and Marchiori M., 2001, Physical Review Letter 87:19, *Efficient behaviour of small-world networks*

Moreira A., Andrade J., Herrmann H. and Indekeu J., 2008, arXiv:0812.3591v1, *How to make a fragile network robust and vice versa*

Newman M.E.J., 2001, Physical Review E 64, *Scientific collaboration networks I. Network construction and fundamental results & Scientific collaboration networks II. Shortest paths, weighted networks and centrality*

Newman M.E.J., Barabasi A.-L. and Watts D., 2006, *Structure and Dynamics of networks*

Redner S., 1998, Eur. Phys. J. B. 4, 131-134, *How popular is your paper? An empirical study of the citation distribution*

Scala A., Amaral L.A.N. and Barthelemy M., 2000, Eur. Phys. Letter 55, 594, *H.E. Classes of behaviour of small-world networks*.

Watts D.J. and Strogatz S.H., 1998, Nature 393, 440, *Collective dynamics of `small-world' networks*