Journal of Reliability and Statistical Studies; ISSN (Print): 0974-8024, (Online):2229-5666
Vol. 6, Issue 1 (2013): 01-09

COMPARING RANDOM AND REGULAR NETWORK RESILIANCE AGAINST RANDOM ATTACK ON THEIR NODES

Ilya B. Gertsbakh[1] and Yoseph Shpungin[2]

[1]Department of Mathematics, Ben-Gurion University, P.O.Box 653, Beer-Sheva 84105, Israel
[2]Software Engineering Department, Sami Shamoon College of Engineering, Beer-Sheva 84100, Israel
Email: elyager@bezeqint.net; yosefs@sce.ac.il

(Received April 09, 2012)

Abstract

We consider a family of connected networks whose nodes are subject to random failures ("attacks"). Node failure means elimination of all links incident to the attacked node. Each node, independently of others, fails with probability q . Network failure (*DOWN*) state is defined as the situation when the largest connected component has "critical" size $\le L$. We compare the probabilistic resilience of a simulated network (obtained by a preferential assignment-type algorithm) versus a regular network having the same number of nodes and links. This comparison is carried out for three types of regular networks: the dodecahedron (20 nodes, 30 links), square torus-type grid (25 nodes, 50 links) and five-dimensional cubic network (32 nodes, 80 links). For all three types of networks the critical value of L was approximately equal one third of the nodes. It turns out that the network with regular structure and node degree $d=5$ has higher resilience than a network with random structure, i.e. a regular network has smaller *DOWN* probability than a random network for the same q value and for the same number of failed nodes x It turns out, however, that the advantage of a regular network over a random network vanishes with the decrease of the average node degree. So, for $d=3$, random network and its regular counterpart (so-called dodecahedron) have approximately the same resilience. Our investigation is based on comparing the so-called cumulative D-spectra and the network *DOWN* probabilities as a function of node failure probability q.

Key words: Cumulative D-spectrum, Dodecahedron, Five-dimensional cube, Maximal connected component, Network resilience, Node degree, Node failures, Preferential assignment, Regular grid.

1. Introduction

1.1. Network and its *UP* and *DOWN* States

By network $\mathbf{N}=(V,E)$ we denote an undirected graph with a node-set V, $|V|=n$, and an edge-set (link-set) E, $|E|=m$. If all nodes of the network are connected to each other directly or indirectly, the network is called connected. A nonempty subset of nodes $V_1 \subset V$ connected to each other by a set of edges (links) $E_1 \subset E$ is called *isolated component* (or simply - component) of the network if there are no edges of type $e=(a,b)$, where $a \in V_1$ and $b \in V-V_1$. The size of the component is defined as the number of its nodes.

Network elements subject to failures are the nodes. A node can be in two states, *up* and *down*. Node v failure (*down*) means elimination of all links having v as their end node, while the node itself remains to exist. All nodes have failure probability q and fail independently of each other. It is assumed that initially $\mathbf{N}=(V,E)$ is connected, i.e. there is one component of size *n*; nodes fail (are "attacked") in random order, according to a "lottery" in which each node has failure probability *q*. As a result, network disintegrates into connected components of smaller size. Network may enter the *DOWN* state which, by definition, means that the largest component has size not exceeding the "critical" number *L*. Network *UP* state is, by definition, the complement to the *DOWN* state.

1.2. D-spectrum of the Network

The central role in our exposition belongs to the method of computing the network *DOWN* probability as a function of the number of nodes failed in the network. This probability is expressed via so-called *D-spectrum*, see Gertsbakh and Shpungin (2009). ("D" -stands for destruction).

Suppose that we number the nodes from 1 to *n* and consider a *random permutation* $\pi=\{i_1,i_2,...,i_n\}$ of their numbers. We assign equal probability $1/n!$ to each permutation. Imagine that initially all nodes are *up* and we turn them *down* one-by-one by moving along π from left to right. The first node i_r such that the network becomes *DOWN* when the *r*-th node in π gets *down* is called the *anchor* of π. D-spectrum is the discrete distribution function of the anchor position. Formally, the D-spectrum is the collection of nonnegative numbers $\{f_1, f_2,..., f_n\}$, where

$$f_r = P(\text{anchor position is r}), r=1,...,n, \sum_{r=1}^{n} f_r = 1. \quad (1)$$

The readers working in reliability who are familiar with so-called coherent system *signatures*

$$\{s_1,s_2,...,s_n\},$$

see, e.g. Samaniego (1985, 2007), will realize that $s_r = f_r$, $r=1,...,n$. Elperin et al (1991) introduced it under the name *ID* (*Internal Distribution*) of the system.

We will need also the *cumulative* D-spectrum $F(x)$:

$$F(x)=\sum_{r=1}^{x} f_r, x=1,...,n. \quad (2)$$

Obviously, $F(n)=1$. By its definition, $F(x)$ equals the probability that the network is *DOWN* when x of network nodes are *down*.

So far nodes failures appeared in the artificial process of network "destruction". Now suppose that each node can be in two states, *up* and *down*, and each node, independently of other nodes, will be *up* with probability *p* and *down* with probability $q = 1 - p$. Note that elementary arguments lead to the following formula for $P(DOWN)$:

$$P_q(DOWN) = \sum_{x=1}^{n} C(x) q^x p^{n-x}, \qquad (3)$$

where $C(x)$ is the number of network failure (cut) sets with exactly x nodes in the *down* state and $(n-x)$ nodes - in the *up* state.

In further exposition we will use the following important relationship connecting $C(x)$ with $F(x)$:

Claim

$$C(x) = F(x)\frac{n!}{x!(n-x)!}. \qquad (4)$$

We omit the proof of (4). This claim establishes a purely combinatorial fact since the random mechanism leading to $F(x)$ does not depend on *p,q*. The proof of (4) can be found, for example, in Gertsbakh and Shpungin (2009), Chapter 8.

1.3. Description of Networks

In this paper we compare the nodal resilience of three types of networks differing by their average node degree.

A. The first type are the networks with node degree $d = 5$ and $n = 32$ nodes having the same number of links $m = 80$. For this type of networks we compare the regular 5-dimensional cubic network H_5 with a family of three random networks having the same number of nodes and links, and having therefore the same average node degree $\bar{d} = 5$. Each of these random networks is obtained by applying the so-called preferential assignment algorithm, suggested by Barabasi and Albert (1999). This method is supposed to reproduce the natural growth of a network with a strongly nonuniform degree distribution and with the appearance of several nodes ("hubs") having high number of incident links. Construction of a network by this algorithm starts with a "kernel" network $N_0 = (V_0, E_0)$ having a small number of nodes $|V_0| = n_0$ and several links $m_0 = |E_0|$. On each step of the construction, a new node *v* with *d* links is added to the existing network, and the probability that *v* will be connected by a link to an existing node *w* is proportional to the degree d_w of node *w*. We carried out this construction adding on each step a new node and $d = 5$ links, to obtain a network with 32 nodes and exactly 80 links.

We simulated three independent replicas of networks of this type which we call $H-1$, $H-2$ and $H-3$. These networks typically have several "hubs" of degree 7, 8, 9 and a large number of nodes having small degree $d = 1$ or $d = 2$.

To understand the structure of the regular 5-dimensional cube network $H-5$ let us note that the nodes in it are numbered by 5-digit binary numbers ranging from (0,0,0,0,0) to (1,1,1,1,1), and each node is connected to five other nodes whose binary number differs by a single digit. So, for example, the node (0,0,0,0,0) is incident to five nodes (1,0,0,0,0), (0,1,0,0,0), (0,0,1,0,0), (0,0,0,1,0) and (0,0,0,0,1). Cubic networks have some optimal properties in the process of information delivery between nodes, see Mitzenmaher and Upfall (2005) and because of that they are often used as a frame for connecting computer stations (nodes) into a computer network. For all networks of type **A** the critical number $L=10$.

B. The second family of networks has node degree $d=4$. Its regular representative is a square torus-type network *GRID* with 5x5=25 nodes. Let us describe shortly the structure of this network. It is a planar 5x5 grid, whose internal nodes have degree $d=4$. Suppose that we number the corner nodes (clockwise) as 1,2,3,4. To achieve degree 4 for these nodes we add two links to each corner. For example, two links are added, connecting nodes 1 and 2 and 1 and 4. In a similar way, we add one extra link ("vertical" or " horizontal") to each border non-corner node connecting them to a symmetric node on the opposite border.

Random counterparts of GRID are three independent replicas of networks, each having 25 nodes and 50 edges. These replicas have been obtained by preferential assignment (PA) algorithm, in which one new node and four new edges were added on each step of creating the network. Let us call the networks of type **B** *Grid* networks and denote the random replicas as $G-1$, $G-2$ and $G-3$. For **B**-type networks the critical number $L=8$, i.e. slightly below one third of the number of nodes. Let us note, that if the PA algorithm produced a non connected network, the construction was repeated until it gave a connected network.

C. The third family consists of networks with average node degree $\bar{d}=3$. The regular representative is so-called dodecahedron network. It has 20 nodes and 30 links, see Gertsbakh and Shpungin (2009), p.66, Fig.4.2. The random counterparts of this network (denoted as $D-1$, $D-2$ and $D-3$) are three random replicas of networks obtained by applying the above described PA algorithm in which exactly three edges were added to the growing network on each stage of the algorithm. Of course, non connected exemplars produced by PA algorithm were neglected. For type **C** networks, the critical component size was taken $L=7$, again close to one third of the number of nodes.

Remark. Central role in our study is played by the cumulative network D-spectra. The exact calculation of the D-spectrum is an NP-complete problem. We are using an *approximation* to the D-spectrum which is based on a Monte Carlo (MC) simulation. The main part of the MC procedure is generating one replica of random node number permutation π and of step-by-step follow up of the network maximal component size in the process of sequential node "destruction". The so-called disjoint set structure (DSS) (see Cormen, 2001) suits ideally for implementing this procedure. For each type of the above described networks the network *DOWN* state was defined as the situation when the maximal connected component is $\leq L$, where L was taken 10, 8, and 7, for type **A,**

B and **C**, respectively. Generation of $M = 10^5$ random permutations allows obtaining sufficiently accurate estimates of the D-spectra for the above described networks.

2. Network D-spectra and DOWN Probability

2.1. Type A Networks

Fig. 1 presents the graphs of the cumulative D-spectra for $H-5$ (the thick curve) and random replicas $H-1, H-2, H-3$ (thin lines).

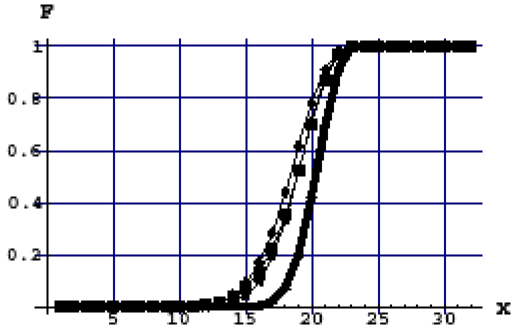

Fig. 1: The D-spectra of $H-5$ (thick) and $H-1, H-2, H-3$ (thin).

Two properties of the spectra presented in Fig. 1 are important. First, the spectra of the random replicas $H-1, H-2, H-3$ are rather close to each other, and second **-** all they clearly lie above the D-spectrum of $H-5$ for *x* ranging from 10 to 23, in which the spectra curves change from zero to almost 1. Obviously, the regular cubic network is more resilient than its random counterparts.

This becomes more obvious if we compare the corresponding probabilities that the network is in *DOWN* state for various node failure values *q*, see Table 1.

For example, for $q = 0.5$, the probability that the regular network is *DOWN* equals $P_{0.5}(H_5) = 0.095$ while for the random counterparts of this network the corresponding probability ranges from 0.165 to 0.195, which is a considerable increase and signifies smaller resilience of random networks.

On the early stage of our research, which we have reported in Gertsbakh and Shpungin (2011), we did not carry out similar comparisons for networks having smaller number of node degree. Moreover, we were convinced that the same advantage of a regular network over its random counterpart will remain true for $d = 4$ and $d = 3$. The real picture however, turns out to be different, as it can be seen from the next subsection.

q	$P_q(H-1)$	$P_q(H-2)$	$P_q(H-3)$	$P_q(H_5)$	$P_q(H_5;MPA)$
0.40	0.029	0.036	0.039	0.010	0.054
0.45	0.076	0.085	0.095	0.036	0.119
0.50	0.165	0.176	0.195	0.095	0.226
0.55	0.304	0.314	0.343	0.209	0.377
0.60	0.485	0.490	0.525	0.380	0.556
0.65	0.676	0.677	0.709	0.585	0.731
0.70	0.836	0.835	0.857	0.777	0.870
0.80	0.985	0.984	0.987	0.977	0.989

Table 1: *DOWN* probability of $H-5$ and its random counterparts as a function of *q*

2.2. Type B and C Networks

Fig. 2 presents the spectra of three random networks $G-1, G-2, G-3$ (thin curves) and the regular grid network *GRID* (bold curve).

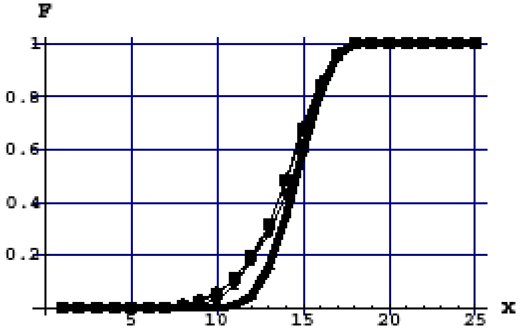

Fig. 2: The D-spectra of *GRID* (thick) and $G-1, G-2, G-3$ (thin).

This figure is similar to the previous one, with the difference being that the bold curve (for *GRID*) is dominated by thin curves only for $x \le 15$ and $F(x) \le 0.6$. For $x > 15$, all spectra practically coincide.

This is confirmed by the data on comparing network *DOWN* probabilities presented in Table 2.

Q	$P_q(G-1)$	$P_q(G-2)$	$P_q(G-3)$	$P_q(GRID)$	$P_q(GRID; MPA)$
0.30	0.017	0.025	0.019	0.006	0.027
0.40	0.088	0.110	0.092	0.057	0.119
0.50	0.274	0.312	0.277	0.240	0.327
0.55	0.485	0.490	0.525	0.380	0.471
0.60	0.574	0.611	0.570	0.562	0.625
0.70	0.853	0.873	0.846	0.858	0.870
0.80	0.981	0.984	0.979	0.983	0.985

Table 2: *DOWN* probability of *GRID* and its random counterparts as a function of *q*

It is seen from this table that the regular *GRID* has smaller *DOWN* probability in the range $q \le 0.6$ only and the advantage of *GRID* over $G-1, G-2, G-3$ is much smaller than the respective advantage of $H-5$ over its random counterparts. Extrapolating this comparison to the situation with dodecahedron network $d=3$ one can expect that the regular network and its random counterparts behave in a similar way. This is confirmed by Fig. 3.

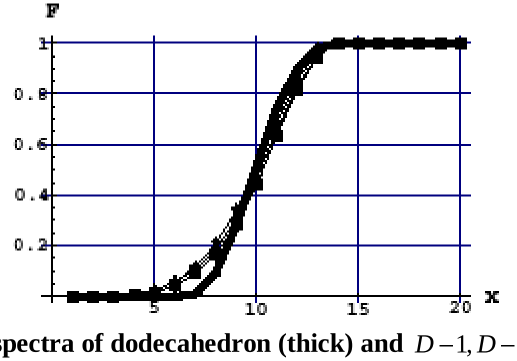

Fig. 3: The D-spectra of dodecahedron (thick) and $D-1, D-2, D-3$ (thin).

Here the regular network (with $d=3$) is slightly more reliable for $x \le 8$ than the random networks (which have almost identical spectra) and is *less reliable* for $x > 8$.

Thus the main conclusion of the above data is that the higher resilience of regular networks over their random counterparts with the same average node degree takes place for $d=5$, and vanishes with the decrease of *d* and does not exist at all for $d=3$.

2.3. Modified PA algorithm and networks with "large" hubs

In Gertsbakh and Shpungin (2011) we compared the regular $H-5$ grid with a random grid obtained by PA algorithm and a slightly modified network describing the 9/11 terrorist network (*Ternet*). *Ternet* had a few very large hubs considerably exceeding by their size the largest hubs which might have been produced by the PA algorithm. It turned out that that *Ternet* was considerably less resilient than its analogue produced by PA algorithm (we called it *Prefnet*), which, in turn, was less resilient than the regular $H-5$ grid.

To generate networks with large hubs we modified the PA algorithm. Our modified preferential assignment (MPA) algorithm works as follows. We produce randomly a "skeleton" of network which consists of its spanning tree with a several extra links. Then the node degrees $d_i, i=1,...,n$ are counted and node *i* gets weight $w_i = d_i^4$. Then the missing links (a,b) are added one-by-one in such a way that one node for each links (say *a*) was chosen randomly and another node went to node *b* with probability proportional to the weight w_b of node *b*. As it has been expected, MPA algorithm produced connected networks with a few very large hubs. For example, three simulated networks with 32 nodes and 80 edges had hubs of size (16,15), (16,14) and (20,16), respectively.

Similar to the case of *Ternet*, MPA produced analogues of $H-5$ which turned out to be considerably less resilient than their counterparts produced by PA. The last column of Table 1 gives the corresponding *DOWN* probabilities (denoted $P_q(H_5; MPA)$).

The situation with Grid network produced by MPA is similar, see the corresponding failure probabilities in the last column of Table 2. However, the difference in P_q between the grids produced by PA and MPA are smaller than in the $H-5$ case.

The advantage in $P_q(DOWN)$ the regular dodecahedron network over its random counterparts produced by MPA is very small and calculations show that it is preserved only for $q=0.3-q=0.4$ and is only of magnitude about 0.05.

References

1. Barabasi, A. and Albert, R. (1999). Emergence of scaling in random networks, Science, V. 286, No. 5439, p. 509-512.
2. Cormen, T. (2001). Introduction to Algorithms, MIT Press.
3. Elperin,T., Gertsbakh, I. and Lomonosov, M. (1991). Estimation of network reliability using graph evolution models, IEEE Transactions on Reliability, TR-40, p. 572-581.
4. Gertsbakh, I. and Shpungin, Y. (2009). Models of Network Reliability: Analysis, Combinatorics and Monte Carlo. CRC Press.
5. Gertsbakh, I and Y. Shpungin (2011). Probabilistic description of network behavior under random attack on its nodes, Proc. of the International Conference on Risk Analysis, ICRA4, p. 105-112.

6. Gertsbakh, I and Y. Shpungin (2011). Network Reliability and Resilience, Springer Briefs in Electrical and Computer Engineering, Springer.
7. Mitzenmacher, M. and Upfal, E. (2005). Probability and Computing, Cambridge University Press.
8. Samaniego F. (1985). On closure of the IFR class under formation of coherent systems, IEEE Transactions on Reliability Theory, TR-34, p. 69-72.
9. Samaniego, F. (2007). System Signatures and Their Application in Engineering Reliability, Springer.