Random Graphs' Robustness in Random Environment

Marina Leri

Institute of Applied Mathematical
Research, Karelian Research Centre,
Russian Academy of Sciences

Yury Pavlov

Institute of Applied Mathematical
Research, Karelian Research Centre,
Russian Academy of Sciences

Abstract

We consider configuration graphs the vertex degrees of which are independent and follow the power-law distribution. Random graphs dynamics takes place in a random environment with the parameter of vertex degree distribution following uniform distributions on finite fixed intervals. As the number of vertices tends to infinity the limit distributions of the maximum vertex degree and the number of vertices with a given degree were obtained. By computer simulations we study the robustness of those graphs from the viewpoints of link saving and node survival in the two cases of the destruction process: the "targeted attack" and the "random breakdown". We obtained and compared the results under the conditions that the vertex degree distribution was averaged with respect to the distribution of the power-law parameter or that the values of the parameter were drawn from the uniform distribution separately for each vertex.

Keywords: random graphs, random environment, power-law distribution, robustness, simulation modeling, forest fire model.

1. Introduction

Recently, random graphs have been widely used for modeling complex networks such as the Internet, social, transport or telecommunication networks (see, e.g., Durrett 2007). One of the random graph models showing its best fit is a so called configuration graph (Bollobas 1980). Real data observations showed (Faloutsos, Faloutsos, and Faloutsos 1999; Durrett 2007) that their topology can be adequately represented by configuration graphs with vertex degrees being independent identically distributed (i.i.d.) random variables possessing natural values. Let ξ be a random variable equal to the degree of any vertex. In (Reittu and Norros 2004) the authors showed that in modeling of huge networks it is more appropriate to use the following vertex degree distribution of the random variable ξ:

$$\mathbf{P}\{\xi = k\} = k^{-\tau} - (k+1)^{-\tau}, \tag{1}$$

where $k = 1, 2, \ldots, \tau > 0$. This distribution is known as a power-law vertex degree distribution, and, moreover, many authors note that in real networks the value of the parameter

τ usually lies in the interval $(1, 2)$ (see, e.g., Faloutsos *et al.* 1999; Reittu and Norros 2004; Durrett 2007). However other values of the parameter τ are not without interest. Thus, for example, it turned out that configuration graphs with vertex degree distribution (1) could be used for modeling forest fires, where $\tau > 2$ is even more important (see, Leri and Pavlov 2014, 2016).

Each vertex degree equals the number of stubs or semiedges coming from it, i.e. the number of edges for which connected vertices are not yet found. All stubs are numbered in an arbitrary order. The sum of vertex degrees has to be even, so if it turns out to be odd, one extra stub is added to an equiprobably chosen vertex. The graph is constructed by joining all stubs one to another pairwise and equiprobably to form edges. Obviously, such graph may contain loops, cycles and multiple edges.

In (Leri and Pavlov 2014, 2016) we studied the robustness of configuration graphs to targeted and random destruction influences. In the case of a random breakdown equiprobably chosen vertices are removed from the graph sequentially with all the incident edges. In the case of a targeted destruction vertices with the highest degrees are removed. We proposed a criterion of graph destruction and found estimates of graph breakdown probability depending on the fraction of removed vertices.

Recently, there appeared some works where the authors note that with growing network size vertex degree distributions of corresponding random graphs may change and even become random variables (see, e.g., Bianconi and Barabasi 2001). Therefore, it was natural to start studying random graphs in random environment, where the vertex degree distribution is not fixed, as in Equation (1), but has a random behaviour.

In (Pavlov 2016) we considered configuration graphs where vertex degrees follow the distribution (1) under the condition that the parameter τ is a random variable uniformly distributed on the interval $[a, b]$, where $0 < a < b < \infty$. Then, the random variable ξ has the following distribution:

$$p_1 = \mathbf{P}\{\xi = 1\} = 1 - \frac{1}{(b - a)\ln 2}\left(\frac{1}{2^a} - \frac{1}{2^b}\right),$$

$$p_k = \mathbf{P}\{\xi = k\} = \frac{1}{(b - a)\ln k}\left(\frac{1}{k^a} - \frac{1}{k^b}\right) - \frac{1}{(b - a)\ln(k + 1)}\left(\frac{1}{(k + 1)^a} - \frac{1}{(k + 1)^b}\right),$$

$$(2)$$

where $k = 2, 3, \ldots$. For such graphs we studied the limit distribution of degree structure for all zones where the number of vertices and the number of edges tends to infinity. New results on the asymptotical behaviour of the vertex degrees are given below.

In this paper we consider the robustness of configuration graphs with random vertex degree distribution. Distribution (2), as well as (1), is the same for all vertices, thus it is not yet a random environment. It is more natural to suppose that vertex degrees are defined by Equation (1), where the value of τ is chosen from the interval $[a, b]$ equiprobably for each vertex (see, Leri 2016). This work includes the results on robustness of both models. Comparison of the results showed their similarity. It means that the study of the graphs' behaviour in the considered random environment can be replaced by the study of the model with an averaged vertex degree distribution (2).

In the next section limit theorems of the maximum vertex degree and the number of vertices of the given degree are proved. Section 3 contains the description of the process of modeling graphs with vertex degree distribution (2). In section 4 we consider graphs in random environment. In section 5 we discuss the results of comparing the negative outcomes of destruction on these two models.

2. Degree structure

Let N be the number of vertices. We denote by $\xi_{(N)}$ and μ_r the random variables equal to the maximum vertex degree and the number of vertices with degree r, respectively. In (Reittu

and Norros 2004) the authors showed that if vertex degrees follow the distribution (1), $\xi_{(N)}$ is proportional to $N^{1/\tau}$ as $N \to \infty$, and μ_r for large r is proportional to $Nr^{-(\tau+1)}$. Let us consider the limit behaviour of these characteristics in the case of vertex degree distribution (2).

Theorem 1. Let $N \to \infty$. Then for any fixed x

$$\mathbf{P}\{a \ln \xi_{(N)} - \ln N + \ln \ln N + \ln(b-a) - \ln a \le x\} \to e^{-e^{-x}}.$$

Proof. Let us denote by $\xi_1, \ldots, \xi_N$ the degrees of vertices $1, \ldots, N$. It is clear that

$$\mathbf{P}\{\xi_{(N)} \le y\} = \mathbf{P}\{\xi_1 \le y, \ldots, \xi_N \le y\} = \mathbf{P}^N\{\xi_1 \le y\}.$$

From this and (2) we obtain that

$$\mathbf{P}\{\xi_{(N)} \le y\} = \left(1 - \frac{1}{(b-a)\ln([y]+1)}\left(\frac{1}{([y]+1)^a} - \frac{1}{([y]+1)^b}\right)\right)^N, \tag{3}$$

where $[y]$ is the integer part of y. It is easy to see that as $y \to \infty$

$$\frac{1}{(b-a)\ln([y]+1)}\left(\frac{1}{([y]+1)^a} - \frac{1}{([y]+1)^b}\right) \sim \frac{1}{(b-a)y^a \ln y}. \tag{4}$$

The theorem assertion follows from (3) and (4) if

$$y = \left(\frac{a}{(b-a)}e^x \frac{N}{\ln N}\right)^{1/a}. \tag{5}$$

Remark 1. From Theorem 1 and (5) we can see that the maximal vertex degree is proportional to $(N/\ln N)^{1/a}$.

Theorem 2. Let $N \to \infty$ and k is a natural number. The following assertions are true.

1. If $Np_r \to \infty$ then uniformly in k such that $u_r = (k - Np_r)/\sqrt{Np_r(1-p_r)}$ lies in any fixed finite interval

$$\mathbf{P}\{\mu_r = k\} = (2\pi Np_r(1-p_r))^{-1/2} e^{-u_r^2/2}(1+o(1)).$$

2. If $r \to \infty$ then uniformly in k such that $(k - Np_r)/\sqrt{Np_r}$ lies in any fixed finite interval

$$\mathbf{P}\{\mu_r = k\} = \frac{(Np_r)^k}{k!} e^{-Np_r}(1+o(1)).$$

Proof. Random variables $\xi_1, \ldots, \xi_N$ are independent, therefore

$$\mathbf{P}\{\mu_r = k\} = \binom{N}{k} p_r^k (1-p_r)^{N-k}. \tag{6}$$

Under the first condition of the theorem $Np_r(1-p_r) \to \infty$ and in (6) we can use the normal approximation of binomial probabilities. Under the second condition $p_r \to 0$ and these probabilities allow Poisson approximation. Straight from here follow assertions of Theorem 2.

Remark 2. Let $r \to \infty$. From (2) we can find that

$$p_r \sim \frac{a}{(b-a)r^{a+1}\ln r}.$$

From here and Theorem 2 it follows that μ_r is proportional to $N/(r^{a+1}\ln r)$.

Remark 3. Let $p_r \to 0$. By Theorem 2 normal and Poisson approximations of μ_r distribution are possible at the same time.

3. Robustness of graphs with given degree distribution

The problem of robustness and vulnerability of present-day huge complex networks to various types of breakdowns remains rather pressing (see, e.g., Bollobas and Riordan 2004; Durrett 2007; Norros and Reittu 2008). Therefore, along with the studies of random graph's structure, we consider the process of its destruction aiming to look at how the main structural characteristics would change with the removal of graph vertices. In this Section we study configuration random graphs with vertex degrees following the distribution (2) on a predefined interval $[a, b]$. We consider two types of the destruction process. During the first one (link saving) we remove graph vertices sequentially with all the incident edges. The aim is to consider changes of the graph structure with vertex removal. The second process (node survival = forest fire model) takes the similarity with the process of fire spreading (it could also be any other destructive influence (Arinaminparthy, Kapadia, and May 2012; Bertoin 2011, 2012; Drossel and Schwabl 1992)), where the destruction starts from a chosen vertex and then spreads over the graph through its edges in some certain way. For each type of destruction process we consider two cases: "targeted attack" means the removal of vertices with the highest degrees (link saving) or "targeted lightning-up" of a vertex with the highest degree (node survival) on the one hand, and "random breakdown" – the removal of equiprobably chosen vertices (link saving) or "random ignition" of an equiprobably chosen vertex (node survival) on the other. The main method of studies described below is simulation modeling followed by statistical analysis of the obtained data.

3.1. Link saving: preserving graph connectivity

The first considered graph destruction process – link saving – was done on simulation models of graphs sized from 1000 to 10000 vertices and three intervals $[a, b]$: $(1, 2)$, $(1, 3]$ and $[2, 3]$. Power-law configuration graphs with the parameter $\tau \in (1, 2)$ are known to be a good representation of the AS-level topology, where AS means autonomous systems (see, e.g., Faloutsos *et al.* 1999; Mahadevan, Krioukov, Fomenkov, Huffaker, Dimitropoulos, Claffy, and Vahdat 2006; Reittu and Norros 2004). Power-law graphs with the parameter $\tau \in [2, 3]$ are useful for the studies of forest fire models (Leri and Pavlov 2014, 2016; Leri 2016). The interval $(1, 3]$ is chosen as a generalization. The purpose is to estimate the graph breakdown probability depending on the percentage of removed vertices.

Let random variables $\eta_1, \eta_2, \ldots, \eta_s$ be equal to the percentages of vertices in the graph components in decreasing order. Thus η_1 is the percentage of vertices in the largest component, η_2 – the percentage of vertices in the second-sized component, etc., where s is the number of graph components. In (Leri and Pavlov 2014) we proposed the criterion of graph destruction to be the occurrence of the following event A : $\{\eta_1 \leq 2\eta_2\}$, which means that the percentage of vertices in the largest component becomes less than or equal to the two values of the percentage of vertices in the second largest component. This criterion is suggested because the largest components of the considered graphs are far larger than their second components. The average initial ratios of the sizes of the first two largest components of the considered graphs depend on the graph size N as follows: $\eta_1/\eta_2 = 0.15N + 81$ for $(1, 2)$; $\eta_1/\eta_2 = 0.002N + 7.7$ for $[2, 3]$; $\eta_1/\eta_2 = 0.08N + 50$ for $(1, 3]$, where determination coefficients R^2 of all these regression models are equal to 0.99. This means that, for example, when $[a, b] = (1, 2)$ the ratio η_1/η_2 is more than 200 for $N = 1000$ and more than 1600 for $N = 10000$.

In Figures 1 and 2 we plot the following regression relations between the probabilities $\mathbf{P}\{A\}$ of graph destruction, the percentage of vertices removed from the graph r and the initial graph size N. For the process of targeted attack on vertices with the highest degrees we obtained

the following regression models:

$$\mathbf{P}\{A\} = -0.47 + 0.054r^{1.9} + 0.046 \ln N, \qquad (1,2), \qquad (R^2 = 0.96)$$
$$\mathbf{P}\{A\} = 0.26 + 0.31 \ln r + 0.1 \ln N, \qquad [2,3], \qquad (R^2 = 0.99)$$
$$\mathbf{P}\{A\} = -0.63 + 0.27r^{1.3} + 0.06 \ln N, \qquad (1,3), \qquad (R^2 = 0.95)$$

where the value of r is limited as follows: $4.21 - 0.354 \ln N \leq r \leq 5.75 - 0.108 \ln N$ for $(1,2)$, $0.115 - 0.01 \ln N \leq r \leq 2.89 - 0.256 \ln N$ for $[2,3]$ and $2.24 - 0.2 \ln N \leq r \leq 4.03 - 0.122 \ln N$ for $(1,3)$. In practice, it is clear that for the out-of-limits values of r the probability $P\{A\} = 0$ when r is less than the lower limit and $P\{A\} = 1$ when r is larger than the upper limit. The same is true for the models given below. In the case of random breakdowns the relations are as follows:

$$\mathbf{P}\{A\} = -0.4 + 0.00035r^2 - 0.04 \ln N, \qquad (1,2), \qquad (R^2 = 0.92)$$
$$\mathbf{P}\{A\} = 0.51 + 0.02r - 0.07 \ln N, \qquad [2,3], \qquad (R^2 = 0.99)$$
$$\mathbf{P}\{A\} = -0.45 + 0.00041r^2 - 0.04 \ln N, \qquad (1,3), \qquad (R^2 = 0.92)$$

with the following limits for r: $35.32 + 1.25 \ln N \leq r \leq 63.59 + 0.81 \ln N$ for $(1,2)$, $0.056 + 0.00074N \leq r \leq 24.5 + 3.5 \ln N$ for $[2,3]$ and $34.36 + 1.12 \ln N \leq r \leq 59.77 + 0.74 \ln N$ for $(1,3)$.

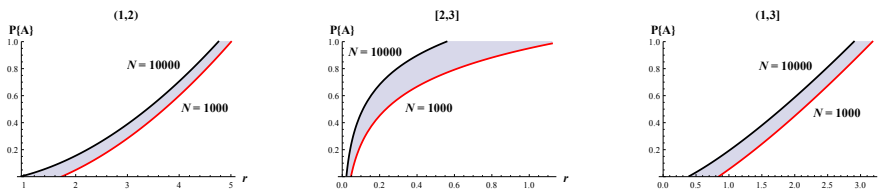Figure 1: Probability of graph destruction in the case of targeted attacks on graphs with $[a,b] = (1,2)$, $[2,3]$ and $(1,3)$, respectively.
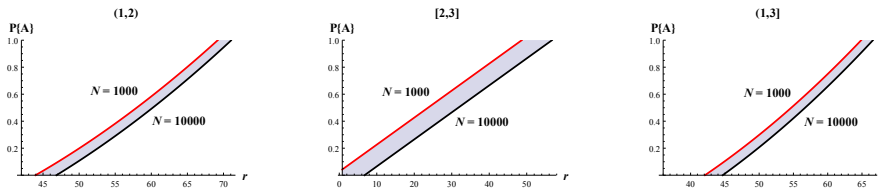

Figure 2: Probability of graph destruction in the case of random breakdowns of graphs with $[a,b] = (1,2)$, $[2,3]$ and $(1,3)$, respectively.

The dependencies for $1000 < N < 10000$ fall within shaded regions. Simulation results show that configuration graphs with vertex degree distribution (2) are more robust to random breakdowns than to targeted attacks on the vertices with the highest degrees. To destroy such a graph by removing vertices with high degrees it is enough to take away $1 - 5\%$ of them. However, in the case of random vertex removal, the graph will be ruined by the destruction of $50 - 70\%$ of its vertices. Thus, in the case when $[a,b] = [2,3]$ graphs are more vulnerable to both targeted and random breakdowns than in the cases when $[a,b] = (1,2)$ and $[a,b] = (1,3)$.

3.2. Node survival: forest fire model

The study of a destruction process which is called a forest fire model imposes some constraints on the graphs being considered. Since we view graph vertices as trees growing in a limited area of a real forest, their number as well as the number of vertices in a corresponding graph has to

be limited. Thus, we propose to use an auxiliary square lattice graph of the size 100×100 (Leri 2016; Leri and Pavlov 2016). Two vertices of the graph are connected if on the corresponding tree topology a fire can move from one tree to another. We consider 15 different relative allocations of edges and vertices on our lattice graphs. Let m be an averaged inner vertex degree. For a fully packed square lattice $m = 8$. Then for each lattice graph topology we calculated corresponding values of m and N. Let the size of our power-law configuration graph be equal to the size of the auxiliary lattice graph. Knowing that $m = \zeta(\tau)$ (where $\zeta(x)$ is the Riemann zeta function), we obtained a regression relation between the power-law configuration graph size $N \leq 10000$ and the parameter τ of vertex degree distribution (1) (see Figure 3):
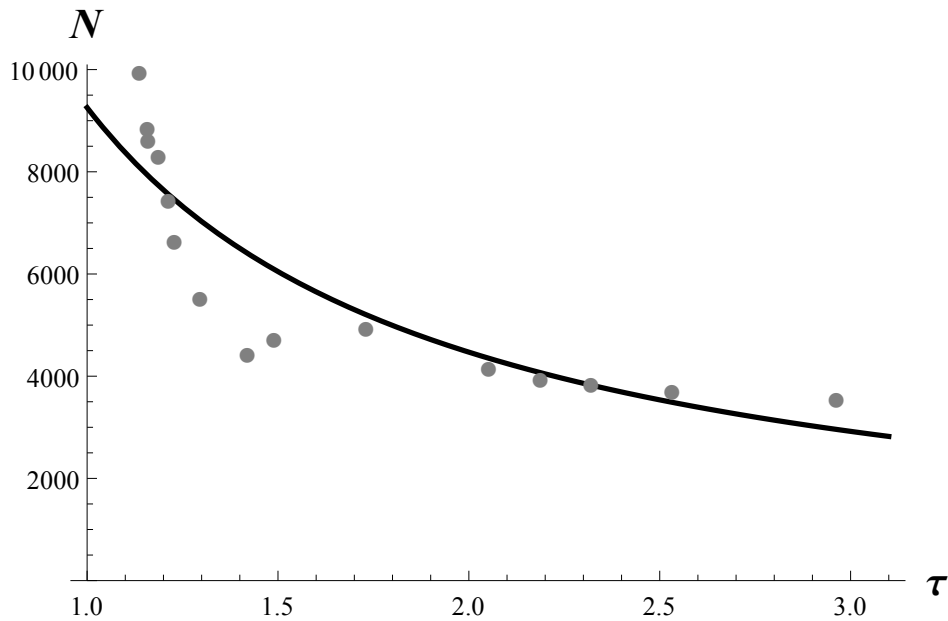
$$N = [9256\tau^{-1.05}], \qquad R^2 = 0.97. \tag{7}$$

Figure 3: Regression relation between N and τ.

Let $\bar{\tau} = (a + b)/2$, then the relation (7) confines the number of vertices N in a corresponding power-law graph. Here, as in Subsection 3.1, we consider the same three intervals $[a, b]$: $(1, 2)$, $[2, 3]$, $(1, 3)$ with the N values obtained from (7) being equal to 6046, 3536 and 4470, respectively. As it was mentioned above, we analyse two cases of starting a fire propagation process: targeted lightning-up and random ignition. When the fire starts it spreads through the incident edges to connected vertices with the probability of fire transition p. This probability could be either a predefined value $p \in (0, 1]$ fixed for all the graph edges or a random variable following the standard uniform distribution. Here we study both cases. The purpose is to find the optimal interval $[a, b]$ of the distribution (2) that would ensure maximum survival of graph vertices in case of a fire. For all the three intervals we found relations between the average number of vertices surviving in a fire n and the probability of fire transition p. Plots on Figure 4 show how the number of remaining vertices n depends on the probability p in the two fire-start cases: targeted lightning-up (left plot) and random ignition (right plot).

It is clear that with the increase of the probability p the number of remaining vertices n will be decreasing. Furthermore, at lower values of p graphs with $[a, b] = (1, 2)$ prove to be more resilient to the fire destruction process in both cases of fire start. But as the value of p increases the topology with $[a, b] = [2, 3]$ will ensure a better survival of graphs vertices. As for graphs with $[a, b] = (1, 3)$, they are the most vulnerable to this kind of destruction in both fire-start cases.

Further we consider the probability of fire transition p to be a random variable drawn from the standard uniform distribution. Table 1 shows an average number of vertices having remained
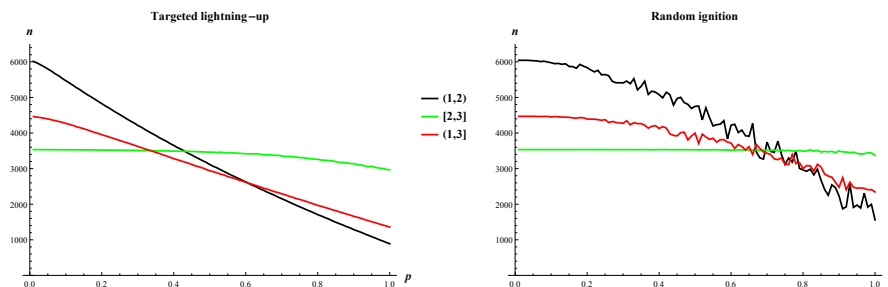
Figure 4: Relation between the number of surviving vertices n and the probability of fire transition.

in the fire for the three considered intervals and the two fire-start cases.

Table 1: Average number of nodes surviving in a fire $\overline{n}$.

$[a,b]$	targeted lightning-up	random ignition
$(1,2)$	3122	4605
$[2,3]$	3471	3531
$(1,3]$	2950	3959

Thus, when the fire starts from a vertex with the highest degree more vertices will survive on the graph topology with the vertex degree distribution (2) with $[a,b] = [2,3]$. But in the case of random ignition graphs with $[a,b] = (1,2)$ will be more resilient to the fire.

4. Graphs' robustness in random environment

In this Section, as distinct from Section 3, vertex degrees of the considered configuration graphs follow the distribution (1), where $\tau \sim \mathbf{U}[a,b]$, which means that the parameter τ is uniformly distributed on a predefined interval $[a,b]$ and the values of τ are chosen separately for each vertex. Here we follow the same study scheme as in Section 3, considering the two types of the destruction process: link saving and node survival with the two cases of destruction spreading: targeted and random.

4.1. Link saving: preserving graph connectivity

As before, we consider graphs of the sizes $N \in [1000, 10000]$ and the three intervals $[a,b]$: $(1,2)$, $(1,3]$ and $[2,3]$. Having obtained statistical data from computer simulations we derived regression relations between the probabilities $\mathbf{P}\{A\}$ of graph destruction, the percentage of vertices removed from the graph r and the initial graph size N. The following regression models were obtained in the case of a targeted attack (see Figure 5):

$$\mathbf{P}\{A\} = -0.44 + 0.04r^{2.1} + 0.05 \ln N, \qquad (1,2), \qquad (R^2 = 0.96)$$
$$\mathbf{P}\{A\} = 0.72 + 0.3 \ln r + 0.04 \ln N, \qquad [2,3], \qquad (R^2 = 0.99)$$
$$\mathbf{P}\{A\} = -0.65 + 0.3r^{1.2} + 0.06 \ln N, \qquad (1,3], \qquad (R^2 = 0.95)$$

and in the case of random breakdowns (see Figure 6):

$$\mathbf{P}\{A\} = -0.53 + 0.00033r^2 - 0.016 \ln N, \qquad (1,2), \qquad (R^2 = 0.93)$$
$$\mathbf{P}\{A\} = 0.42 + 0.019r - 0.056 \ln N, \qquad [2,3], \qquad (R^2 = 0.99)$$
$$\mathbf{P}\{A\} = -0.17 + 0.0004r^2 - 0.064 \ln N, \qquad (1,3], \qquad (R^2 = 0.93)$$

with the following limits for r in the case of a targeted attack: $6.91 - 0.745 \ln N \leq r \leq 5.59 - 0.108 \ln N$ for $(1,2)$, $0.064 - 0.00408 \ln N \leq r \leq 1.79 - 0.114 \ln N$ for $[2,3]$ and $2.11 -$

$0.186 \ln N \leq r \leq 4.17 - 0.133 \ln N$ for $(1, 3]$. and in the case of random breakdowns: $40.32 + 0.54 \ln N \leq r \leq 68.15 + 0.34 \ln N$ for $(1, 2)$, $-0.28 + 0.0006N \leq r \leq 30.5 + 3 \ln N$ for $[2, 3]$ and $25.88 + 1.92 \ln N \leq r \leq 55 + 1.23 \ln N$ for $(1, 3]$. It is easy to see that the obtained models are similar in function forms and only slightly differ in regression models' coefficients.
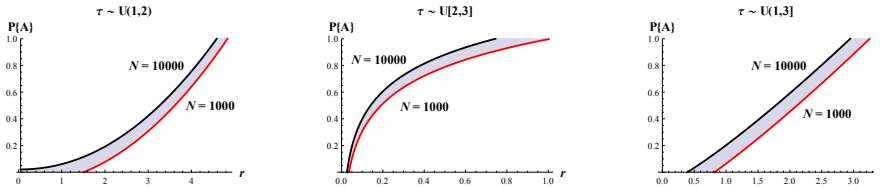

Figure 5: Probability of graph destruction in the case of targeted attacks on graphs with $\tau \sim \mathbf{U}(1, 2)$, $\tau \sim \mathbf{U}[2, 3]$ and $\tau \sim \mathbf{U}(1, 3]$, respectively.
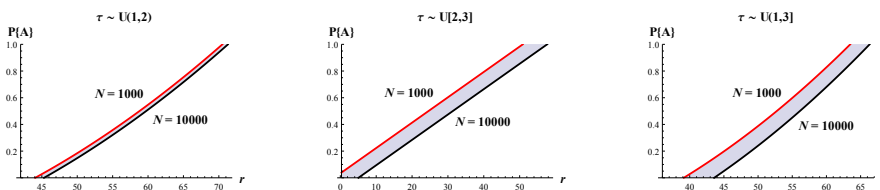

Figure 6: Probability of graph destruction in the case of random breakdowns of graphs with $\tau \sim \mathbf{U}(1, 2)$, $\tau \sim \mathbf{U}[2, 3]$ and $\tau \sim \mathbf{U}(1, 3]$, respectively.

Again, similarly to the graphs with the distribution (2), average initial ratios between the sizes of the first two largest components depend on the graph size N in the following way: $\eta_1/\eta_2 = 0.14N + 100$ for $(1, 2)$; $\eta_1/\eta_2 = 0.002N + 7.1$ for $[2, 3]$; $\eta_1/\eta_2 = 0.08N + 68$ for $(1, 3]$, where $R^2 = 0.99$ for all the three models.

Thus, the considered graphs also proved to be more robust to random breakdowns than to targeted attacks on vertices with the highest degrees. In the case of targeted attack it is enough to remove $1 - 5\%$ of vertices to destroy a graph, and in the case of random breakdowns it takes $50 - 70\%$. Here, like in Section 3, the same notes concerning the smallest values of the removed vertices are true (see Figures 5 and 6). Similarly to the results described in Section 3, in the case when $\tau \sim \mathbf{U}[2, 3]$ graphs are more vulnerable to both targeted and random breakdowns than in the cases where $\tau \sim \mathbf{U}(1, 2)$ and $\tau \sim \mathbf{U}(1, 3]$.

4.2. Node survival: forest fire model

Here we discuss the results of studying forest fire modeling on configuration graphs with the vertex degree distribution (1) and $\tau \sim \mathbf{U}[a, b]$. As in Section 3, we use an auxiliary square lattice graph of the size 100×100 to confine the number of vertices N through the relation (7) with $\overline{\tau} = (a + b)/2$. We consider the same three intervals $[a, b]$: $(1, 2)$, $[2, 3]$, $(1, 3]$ on which the parameter τ is uniformly distributed. The values of N obtained from (7) were the same as in Section 3.2. Again we consider the two fire-start cases: targeted lightning-up and random ignition. The probability of fire transition p is either a predefined value $p \in (0, 1]$ fixed for all graph edges or a random variable following the standard uniform distribution. The aim is to find the optimal interval of the parameter τ that would ensure maximum survival of graph vertices in case of a fire. Plots in Figure 7 show relations between the average number of vertices surviving in a fire n and the probability of fire transition p for the two fire-start cases.

It is quite clear that the obtained results are rather similar to those in Section 3. So are the results for the case where the probability of fire transition p is a random variable uniformly distributed on $(0, 1]$ (see Table 2).
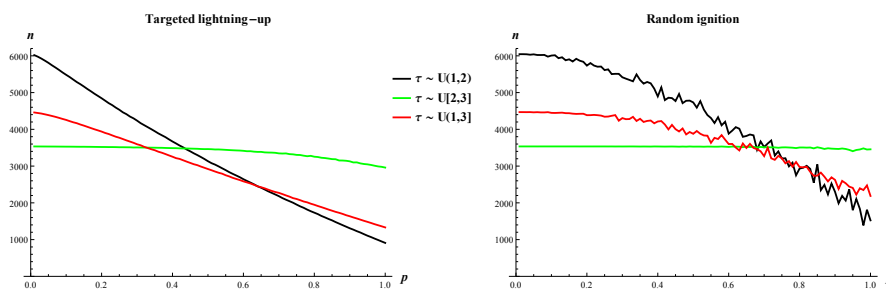
Figure 7: Relation between the number of surviving vertices n and the probability of fire transition.

Table 2: An average number of nodes surviving in a fire $\overline{n}$.

$\tau \sim \mathbf{U}[a, b]$	targeted lightning-up	random ignition
$(1, 2)$	3146	4933
$[2, 3]$	3464	3533
$(1, 3]$	2917	3927

5. Conclusions

The simulation model of the graph destruction process in random environment used in Section 4 is more complicated and requires far more computations than the model with fixed vertex degree distribution (2) in Section 3. At the same time, it is easy to see that the results obtained in Sections 3 and 4 are quite close to each other. This means that we can study the dynamics of random graphs in random environment using averaged degree distributions. But the problem of finding the conditions when such an interchange is incorrect is still open.

6. Acknowledgements

References

Arinaminparthy N, Kapadia S, May R (2012). "Size and Complexity in Model Financial Systems." *Proceedings of the National Academy of Sciences of the USA*, **109**, 18338–18343.

Bertoin J (2011). "Burning Cars in a Parking Lot." *Commun. Math. Phys.*, **306**, 261–290.

Bertoin J (2012). "Fires on Trees." *Annales de l'Institut Henri Poincare Probabilites et Statistiques*, **48**(4), 909–921.

Bianconi G, Barabasi AL (2001). "Bose-Einstein Condensation in Complex Networks." *Physical Review Letters*, **86**, 5632–5635.

Bollobas B (1980). "A Probabilistic Proof of an Asymptotic Formula for the Number of Labelled Regular Graphs." *Eur. J. Comb.*, **1**, 311–316.

Bollobas B, Riordan O (2004). "Robustness and Vulnerability of Scale-free Random Graphs." *Internet Mathematics*, **1**(1), 1–35.

Drossel B, Schwabl F (1992). "Self-organized Critical Forest-fire Model." *Phys. Rev. Lett.*, **69**, 1629–1632.

Durrett R (2007). *Random Graph Dynamics*. Cambridge Univ. Press, Cambridge.

Faloutsos C, Faloutsos P, Faloutsos M (1999). "On Power-law Relationships of the Internet Topology." *Computer Communications Rev.*, **29**, 251–262.

Leri M (2016). "Forest Fire Model on Configuration Graphs with Random Node Degree Distribution." In *XVII-th International Summer Conference on Probability and Statistics: Conference Proceedings and Abstracts*, pp. 29–32.

Leri M, Pavlov Y (2014). "Power-law Random Graphs' Robustness: Link Saving and Forest Fire Model." *Austrian Journal of Statistics*, **43**(4), 229–236.

Leri M, Pavlov Y (2016). "Forest Fire Models on Configuration Random Graphs." *Fundamenta Informaticae*, **145**(3), 313–322.

Mahadevan P, Krioukov D, Fomenkov M, Huffaker B, Dimitropoulos X, Claffy K, Vahdat A (2006). "The Internet AS-Level Topology: Three Data Sources and One Definitive Metric." *ACM SIGCOMM Computer Communication Review (CCR)*, **36**(1), 17–26.

Norros I, Reittu H (2008). "Attack Resistance of Power-law Random Graphs in the Finite Mean, Infinite Variance Region." *Internet Mathematics*, **5**(3), 251–266.

Pavlov Y (2016). "On Conditional Configuration Graphs with Random Distribution of Vertex Degrees." *Transactions of Karelian Research Centre of Russian Academy of Science: Mathematical Modeling and Information Technologies*, **8**, 62–72. In Russian.

Reittu H, Norros I (2004). "On the Power-law Random Graph Model of Massive Data Networks." *Performance Evaluation*, **55**, 3–23.

Affiliation:

Yury Pavlov
Institute of Applied Mathematical Research
Karelian Research Centre
Russian Academy of Sciences
Pushkinskaja,11, Petrozavodsk 185910, Russia
E-mail: pavlov@krc.karelia.ru
URL: http://mathem.krc.karelia.ru/member.php?id=9&plang=e