ON ROBUSTNESS OF CONFIGURATION GRAPHS WITH RANDOM NODE DEGREE DISTRIBUTION

M. M. Leri
Institute for Applied Mathematical Research, Karelian Research Centre of RAS
Petrozavodsk, RUSSIA
e-mail: leri@krc.karelia.ru

Abstract

We consider power-law configuration graphs with node degrees drawn from the power-law distribution with the parameter following the uniform distribution on a chosen interval. By computer simulation we study the robustness of these graphs from a viewpoint of link saving in the two cases of destruction process: the "random breakdown" and the "targeted attack".

1 Introduction

The study of random graphs with node degrees following the power-law distribution continues to attract special interest (see e.g. [3], [5]). The use of such models has been widening with the changes in the structure of massive data networks and with the appearance of new ones. Power-law random graphs used to be considered a good representation of the AS-level topology (see e.g. [4], [7], [9]) and, moreover, variations of these models could be used in other applications. Along with the studies of the structure of present-day complex networks, the problem of their robustness and vulnerability to various types of breakdowns remains rather pressing (see e.g. [2], [3], [8]).

2 Power-law configuration random graph

We consider power-law random graphs with the number of nodes N. Random variables $\xi_1, \xi_2, \ldots, \xi_N$ are independent identically distributed variables drawn from the power-law distribution:

$$\mathbf{P}\{\xi \geq k\} = k^{-\tau}, \qquad \tau > 1,\ k = 1, 2, \ldots. \tag{1}$$

We use the graph construction procedure introduced in [1], where such models were first called configuration graphs. Starting with a predefined number of nodes we draw node degrees from the distribution (1) with the parameter τ following the uniform distribution on a predefined interval $(a, b]$. The node degree gives the number of stubs for each node, numbered in an arbitrary order. Then all the stubs are joined one to another equiprobably forming links. The sum of node degrees has to be even, otherwise one stub is added to a randomly chosen node to form a lacking connection. The graph construction allows loops and multiple links.

3 Robustness in random environment: link saving

The distribution (1) with the parameter $\tau \in (1,2)$ has finite expectation and infinite variance. As the value of τ exceeds 2 the variance of the distribution (1) becomes finite. The power-law configuration graphs with $\tau \in (1,2)$ are known to contain a so-called giant component ([1], [3], [9] etc.) – a connected set of nodes, the number of nodes in which has the expectation proportional to the number of graph nodes N, as $N \to \infty$.

In [6] we considered power-law graphs with the values of the parameter $\tau \in (1,2)$ fixed for each node. With the evolution of networks the value of τ is regarded to change not only within the stated interval $(1,2)$. It may also happen to be a random variable. Therefore here we consider the parameter τ being drawn from the uniform distribution on the interval $(a,b]$. As it was mentioned above the interval $(1,2)$ is interesting due to its application to the Internet graphs and the existence of the giant component. Power-law graphs with the parameter $\tau \in (2,3)$ do not contain the giant component, but are useful for the studies of forest fire models [6]. The interval $(1,3)$ was chosen as a generalization. As in the previous work [6], here we also consider the two types of breakdowns: a "targeted attack" on the nodes with the highest degrees and the "random breakdown" meaning the removal of equiprobably chosen nodes.

To conduct simulations we modeled graphs of the sizes $N \in [1000, 10000]$ with the three ranges of the parameter τ: $(1,2]$, $(1,3]$ and $(2,3]$. The purpose was to look at how the graph structure changes with the destruction of its nodes. Let random variables $\eta_1, \eta_2, \ldots, \eta_s$ be equal to the sizes of graph components in decreasing order, thus η_1 is the percentage of nodes in the largest component, η_2 – the percentage of nodes in the second-sized component, etc. Let s be the number of graph components. Let us consider a graph being destroyed if $\{\eta_1 \leq 2\eta_2\}$, which means that the size of the second largest component becomes greater or equal to half the size of the largest component. Thus we derived the regression relations between the size of the largest component η_1 and the percentage of nodes removed from the graph r. In the case of a "targeted attack" relations were as follows:

$$\begin{aligned}
\eta_1 &= 53.2 - 8.9r - 6.2\ln r, && \tau \in (1,2],\\
\eta_1 &= 31.9 - 7.0r - 9.1\ln r, && \tau \in (1,3],\\
\eta_1 &= -1.3 + 2.5r - 3.9\ln r, && \tau \in (2,3].
\end{aligned}$$

The determination coefficients (R^2) of these regression models are equal to 0.99, 0.98 and 0.96, respectively. For the process of "random breakdowns" we derived the following relations:

$$\begin{aligned}
\eta_1 &= 88.1 - 1.5r, && \tau \in (1,2],\\
\eta_1 &= 73.3 - 1.3r, && \tau \in (1,3],\\
\eta_1 &= 20.2 - 2.7\sqrt{r}, && \tau \in (2,3].
\end{aligned}$$

with determination coefficients 0.97, 0.95 and 0.99, respectively. The results showed that in all cases the graph size N does not affect the size of the largest component. As for the sizes of second-sized components they will diminish slightly with the removal

of graph nodes and will not exceed 20% when $\tau \in (1,2]$, 15% when $\tau \in (1,3]$, and 6% when $\tau \in (2,3]$ of graph nodes. The number of graph components in the case of a "targeted attack" slightly increases with the removal of nodes, although in the case of a "random breakdown" this number decreases.

In Figures 1 and 2 we plot the results of the estimation of the regression relations between the probabilities $\mathbf{P}\{\mathrm{A}\}$ (where A is the following event: $\{\eta_1 \leq 2\eta_2\}$) of graph destruction, the percentage of nodes removed from the graph r and the graph size N.

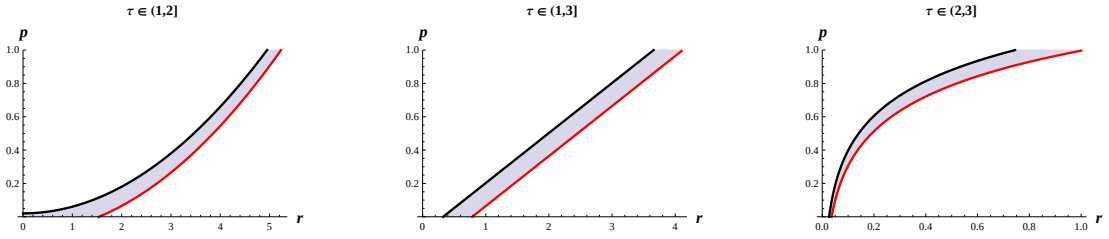

Figure 1: The probabilities of graph destruction in the case of a "targeted attack" (left-hand curve stands for $N = 10000$, right-hand curve – $N = 1000$).

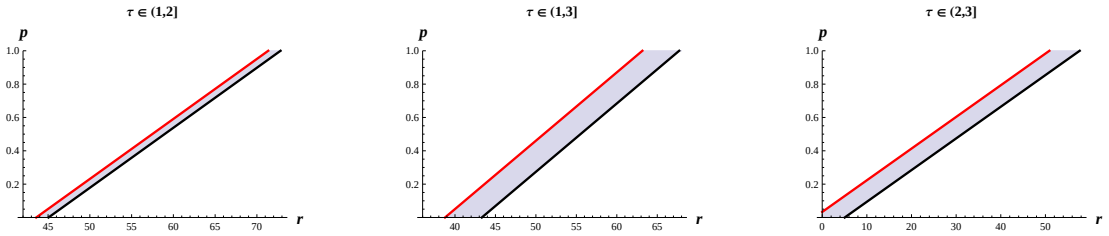

Figure 2: The probabilities of graph destruction in the case of a "random breakdown" (left-hand curve stands for $N = 1000$, right-hand curve – $N = 10000$).

Simulation results showed that power-law configuration graphs are much more robust to "random breakdowns" than to "targeted attacks" on the nodes with the highest degrees. To destroy such a graph by removing nodes with high degrees it is enough to take away $1 - 5\%$ of them. However, in the case of random nodes removal, the graph will be ruined by the destruction of $55 - 75\%$ of its nodes. The obtained results support previous conclusions [6] that the robustness of these graphs strongly depends on the value of the parameter τ. Thus, in the case when $\tau \in (2,3]$ graphs are more vulnerable to both targeted and random breakdowns than in the cases when $\tau \in (1,2]$ and $\tau \in (1,3]$.

4 Acknowledgements

The study is supported by the Russian Foundation for Basic Research, grant 16-01-00005.

References

[1] Bollobas B.A. (1980). A probabilistic proof of an asymptotic formula for the number of labelled regular graphs. *Eur. J. Comb.*. Vol. **1**, pp. 311-316.

[2] Bollobas B., Riordan O. (2004). Robustness and vulnerability of scale-free random graphs. *Internet Mathematics*. Vol. **1**, N **1**, pp. 1-35.

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

[4] Faloutsos C., Faloutsos P., Faloutsos M. (1999). On power-law relationships of the Internet topology. *Computer Communications Rev.*. Vol. **29**, pp. 251-262.

[5] Hofstad R. (2011). *Random Graphs and Complex Networks*. Eindhoven University of Technology.

[6] Leri M., Pavlov Y. (2014). Power-law random graphs' robustness: link saving and forest fire model. *Austrian Journal of Statistics*. Vol. **43**, N **4**, pp. 229-236.

[7] 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)*. Vol. **36**, N **1**, pp. 17-26.

[8] Norros I., Reittu H. (2008). Attack resistance of power-law random graphs in the finite mean, infinite variance region. *Internet Mathematics*. Vol. **5**, N **3**, pp. 251-266.

[9] Reittu H., Norros I. (2004). On the power-law random graph model of massive data networks. *Performance Evaluation*, Vol. **55**, pp. 3-23.