Труды Карельского научного центра РАН
№ 5. 2012. С. 49–53

УДК 519.2

ОБ УСЛОВИЯХ УСТОЙЧИВОСТИ СЛУЧАЙНЫХ ГРАФОВ ИНТЕРНЕТ-ТИПА

М. М. Лери

Институт прикладных математических исследований Карельского научного центра РАН

Рассматриваются случайные графы Интернет-типа, т. е. графы, степени вершин которых имеют степенное распределение с параметром τ из интервала $(1, 2)$. Посредством имитационного моделирования проведен анализ устойчивости этих графов к таким внешним воздействиям, как направленное удаление вершин и равновероятное удаление вершин. Показано, как изменяется структура графа (объемы гигантской и второй по размеру компонент и общее число компонент) с удалением из него вершин в зависимости от объема графа N и значения параметра τ. Получены модели зависимости вероятности разрушения графа от N и τ при обоих условиях внешнего воздействия.

Ключевые слова: случайный граф, имитационное моделирование, устойчивость графа.

M. M. Leri. ON ROBUSTNESS OF POWER-LAW RANDOM GRAPHS

We consider random graphs with vertex degrees being drawn independently from a power-law distribution with parameter τ in the interval $(1, 2)$. By computer simulation we study the resistance of such graphs to «target attacks» such as removal of vertices with the highest degree and to «random breakdowns», i.e. to equiprobable vertex removal. We show how graph structure characteristics (sizes of the giant and the second components, and the number of components) change with vertex deletion depending on the graph size N and parameter τ. The probability of graph destruction depending on N and τ was modeled for both cases.

Key words: random graph, simulation modelling, graph robustness.

С появлением и быстрым развитием глобальных сетей передачи данных, таких как сети телекоммуникаций, телефонные сети и т. п., возрос и продолжает возрастать интерес к изучению их структуры и функционирования [3–8, 10, 11]. Одним из актуальных вопросов является исследование устойчивости этих сетей к такого рода внешним воздействиям, как выход из строя некоторых узлов сети (см., например, [4–6, 10]). Математическим аппаратом, используемым в такого рода исследованиях, являются случайные графы, степени вершин которых являются независимыми одинаково распределенными случайными величинами, распределение которых является дискретным аналогом распределения Парето [7, 11]. В некоторых источниках (см., например, [11] и др.) было высказано предположение, что такие графы могут быть использованы при описании Интернет-топологии (на уровне как доменов, так и маршрутизаторов). Следуя этой интерпретации, такие графы иногда стали

называть графами Интернет-типа (см., например, [2]).

Рассматриваются случайные графы, число вершин которых равно N. Степени вершин графа $\xi_1, \xi_2, \ldots, \xi_N$ являются независимыми случайными величинами, общее распределение которых имеет следующий вид:

$$\mathbf{P}\{\xi \geqslant k\} = k^{-\tau},\ k = 1, 2, \ldots,\ \tau \in (1, 2). \quad (1)$$

В этом случае распределение (1) имеет конечное математическое ожидание и бесконечную дисперсию. При построении графа степени вершин $1, 2, \ldots, N$ являются реализациями случайной величины ξ и определяют различимые полуребра графа (под полуребром понимается ребро, инцидентное некоторой вершине, для которой смежная вершина еще не определена) [11]. Если сумма степеней вершин оказывается нечетной, то равновероятно выбирается вершина графа, степень которой увеличивается на 1. При равновероятном соединении всех полуребер графа образуются ребра. Построенный таким образом граф имеет как петли, так и кратные ребра. Известно [2, 11], что графы Интернет-типа имеют единственную гигантскую компоненту связности, математическое ожидание объема которой пропорционально cN, где $0 < c < 1$ – некоторая положительная постоянная. Теоретические исследования случайных графов Интернет-типа касаются как изучения предельного поведения структурных характеристик таких графов (см., например, [2, 3, 6, 8, 11]), так и исследования их устойчивости к разного рода разрушениям [4–6, 10]. Кроме теоретических подходов, одним из удобных средств изучения случайных графов является имитационное моделирование.

Целью настоящей работы было исследование с помощью метода Монте-Карло устойчивости случайных графов Интернет-типа к процессу разрушения, а именно, к такому внешнему воздействию, как случайное (равновероятное) удаление вершин, а также направленное удаление вершин с большими степенями. Рассматривалось поведение объемов компонент связности графа и их количества в зависимости от процента удаленных из графа вершин при разных значениях параметра распределения степеней вершин графа τ и объема графа N.

Была построена имитационная модель случайного графа Интернет-типа [1] на основе алгоритма, предложенного в [12], с использованием генератора псевдослучайных чисел «вихрь Мерсенна» [9]. С помощью этой модели было показано [1], что структура таких графов главным образом зависит от параметра распределения степеней вершин τ и слабо зависит от фактического объема графа N. Чем ближе значение τ к 1, тем больше доля вершин графа, входящих в гигантскую компоненту (около 95 %), тогда как при значениях τ, близких к 2, в нее входит только чуть более половины всех вершин графа. Что касается объема второй компоненты, то он хоть и несколько увеличивается с ростом значения параметра τ, но, несмотря на это, остается пренебрежимо малым по сравнению с размером гигантской компоненты. При этом существенно возрастает общее число компонент графа. Поэтому были проведены вычислительные эксперименты для графов других размерностей, чем в [1], а именно для значений N от 500 до 5000 с шагом в 500 вершин и для 9 значений параметра τ из отрезка $(1, 2)$ с шагом $0,1$. Для каждого из значений N и τ было сгенерировано по 100 случайных графов. Моделирование графов и имитационные эксперименты проводились на вычислительном кластере КарНЦ РАН. Процесс разрушения графа был представлен следующим образом. Из сгенерированного начального графа на каждом шаге выбиралась одна вершина (либо равновероятно, либо вершина, имеющая наибольшую степень), которая удалялась вместе с выходящими из нее ребрами. Затем вершины, ставшие изолированными, тоже удалялись из графа.

Через $\eta_1, \eta_2, \ldots, \eta_s$ обозначим случайные величины, равные объемам компонент графа и расположенные в порядке убывания (η_1 – объем гигантской компоненты, η_2 – объем второй по размеру компоненты и т. д.), где s – общее число компонент. В качестве критерия разрушения графа будем рассматривать наступление следующего события $A : \{\eta_1 \leqslant 2\eta_2\}$. Таким образом, если объем второй по размеру компоненты графа не меньше, чем половина размера наибольшей компоненты, граф считается разрушенным. По полученным посредством имитационного моделирования статистическим данным с помощью методов регрессионного анализа были оценены следующие зависимости: объема гигантской компоненты η_1 (в %), объема второй по размеру компоненты η_2 (в %) и общего числа компонент s случайного графа Интернет-типа от начального размера графа N, параметра распределения степеней вершин τ и процента удаленных из графа вершин r. При «случайных сбоях» (т. е. при равновероятном удалении вершин графа) получены следующие оценки:

$$\eta_1 = 129 - 36\tau - 1,1r,$$

$$\eta_2 = 2 - 0,25 \ln N + 0,42\tau - 0,017 \ln r,$$

$$\frac{s}{N} = -0,18 + 0,2\tau - 0,004r \ln \tau.$$

Коэффициенты детерминации моделей равны, соответственно, $0,98$, $0,7$ и $0,98$. Приведенные выше модели могут быть использованы при следующих ограничениях на значения процента удаленных из графа вершин: $100/N \leqslant r \leqslant 117 - 32,7\tau$. Здесь и далее ограничение снизу означает удаление из графа одной вершины, а введение ограничения сверху связано с тем, что при удалении большего процента вершин граф уже будет разрушен. Таким образом, при фиксированном τ с ростом процента вершин, удаленных из графа, объем гигантской компоненты η_1 уменьшается линейным образом и не зависит от объема графа, тогда как объем второй компоненты η_2, логарифмически уменьшаясь, в целом не превосходит 2 % от объема графа. А общее число компонент графа с равновероятным удалением из него вершин будет линейно уменьшаться.

Далее рассмотрим результаты, полученные в случае «направленной атаки» (т. е. когда целенаправленно удаляются вершины по одной так, что на каждом шаге исключается вершина с макимальной степенью). Были получены следующие регрессионные зависимости:

$$\eta_1 = 130 - 46\tau - 9r,$$

$$\eta_2 = 4,36 - 0,44 \ln N + \tau + 0,4 \ln r,$$

$$\ln s = -3,3 + \ln N + 2,3 \ln \tau + 0,1r,$$

где коэффициенты детерминации моделей равны, соответственно, $0,95$, $0,6$ и $0,98$, и действует следующее ограничение на процент удаленных вершин: $100/N \leqslant r \leqslant 14 - 5,15\tau$. Это означает, что при фиксированном τ в данном случае, как и при «случайном сбое», получаем линейную зависимость объема гигантской компоненты η_1 от процента удаленных из графа вершин r и здесь также отсутствует зависимость η_1 от объема графа. Объем второй компоненты η_2 тоже, как и при равновероятном удалении вершин, логарифмически уменьшаясь, в целом не превосходит чуть более 4 % от объема графа, а общее число компонент графа с удалением из него вершин экспоненциально возрастает.

Обозначим через p оценку вероятности $\mathbf{P}\{A\}$, где $A : \{\eta_1 \leqslant 2\eta_2\}$. При «случайных сбоях» была получена следующая регрессионная зависимость:

$$p = \begin{cases} 0, & \text{при } r < 37/\sqrt{\tau}, \\ -0,2 + 1,5 \cdot 10^{-4}\tau r^2, & \text{при } 37/\sqrt{\tau} \leqslant r < 89/\sqrt{\tau}, \\ 1, & \text{при } r \geqslant 89/\sqrt{\tau}, \end{cases}$$

где $R^2 = 0,84$. Это означает, например, что оценка вероятности разрушения графа равна 0 при $\tau = 1,1$ для всех $r < 35,3$ %, а при $\tau = 1,9$ для $r < 26,9$ %; и $p = 1$ для $r > 84,8$ % при $\tau = 1,1$, а при $\tau = 1,9$ для $r > 64,5$ %.

В случае же «направленной атаки» зависимость оказалась следующей:

$$p = \begin{cases} 0, & \text{при } \ln r < 1,85 - \tau, \\ -0,38 + 0,06re^{\tau}, & \text{при } 1,85 - \tau \leqslant \ln r \leqslant 3,13 - \tau, \\ 1, & \text{при } \ln r > 3,13 - \tau, \end{cases}$$

где $R^2 = 0,76$. То есть, $p = 0$ при $\tau = 1,1$ для всех $r < 2,12$ %, а при $\tau = 1,9$ для $r < 0,95$ %; и $p = 1$ для $r > 7,6$ % при $\tau = 1,1$, а при $\tau = 1,9$ для $r > 3,4$ %.

Заметим, что имитационные эксперименты показывают, что вероятность разрушения графа как при направленном, так и при случайном воздействиях, не зависит от объема графа. Рассмотрим теперь критические значения вероятностей разрушения графа. В таблицах 1 и 2 приведены эти значения при «направленной атаке» (табл. 1) и при «случайных сбоях» (табл. 2).

Рассмотрим графы, для которых $\tau = 1,1$. Если из такого графа удалять вершины равновероятно, то для того чтобы вероятность разрушения не превысила 5 %, т. е. $\mathbf{P}\{A\} \leqslant 5$ % из него можно удалить не более 38,9 % вершин. Тогда как при целенаправленном разрушении вершин, имеющих максимальную степень на каждом шаге, удаление уже 2,4 % вершин приводит к тому же результату. Заметим, что с ростом значения параметра τ процент вершин, которые могут быть удалены из графа до того, как он может считаться разрушенным, уменьшается. Чтобы полностью разрушить любой граф Интернет-типа с помощью «направленной атаки», достаточно удалить из него чуть менее 8 % вершин, тогда как при «случайных сбоях» граф может быть не разрушен даже при удалении из него 80 % вершин.

Исследование показало, что рассматриваемые случайные графы сильно уязвимы к направленному разрушению, такому как удаление вершин с большими степенями. Но в то же время, они достаточно устойчивы к случайным сбоям, т. е. к такому воздействию, как равновероятное удаление вершин. Что

Таблица 1. Критические значения вероятностей разрушения графа при «направленной атаке»

$p\backslash\tau$	1,1	1,2	1,3	1,4	1,5	1,6	1,7	1,8	1,9
0,01	2,2	2,0	1,8	1,6	1,5	1,3	1,2	1,1	1,0
0,05	2,4	2,2	2,0	1,8	1,6	1,4	1,3	1,2	1,1
0,1	2,7	2,4	2,2	2,0	1,8	1,6	1,5	1,3	1,2
0,5	4,9	4,4	4,0	3,6	3,3	3,0	2,7	2,4	2,2
0,9	7,1	6,4	5,8	5,3	4,8	4,3	3,9	3,5	3,2
0,95	7,4	6,7	6,0	5,5	4,9	4,5	4,0	3,7	3,3
0,99	7,6	6,9	6,2	5,6	5,1	4,6	4,2	3,8	3,4

Таблица 2. Критические значения вероятностей разрушения графа при «случайных сбоях»

$p\backslash\tau$	1,1	1,2	1,3	1,4	1,5	1,6	1,7	1,8	1,9
0,01	35,7	34,2	32,8	31,6	30,6	29,6	28,7	27,9	27,1
0,05	38,9	37,3	35,8	34,5	33,3	32,3	31,3	30,4	29,6
0,1	42,6	40,8	39,2	37,8	36,5	35,4	34,3	33,3	32,4
0,5	65,1	62,4	59,9	57,7	55,8	54,0	52,4	50,9	49,6
0,9	81,6	78,2	75,1	72,4	69,9	67,7	65,7	63,8	62,1
0,95	83,5	79,9	76,8	74,0	71,5	69,2	67,2	65,3	63,5
0,99	84,9	81,3	78,1	75,3	72,7	70,4	68,3	66,4	64,6

касается зависимости устойчивости графов Интернет-типа от изменения значения параметра распределения степеней вершин τ, то оказалось, что как при «направленном», так и при «случайном» удалении вершин, чем ближе значение параметра τ к 1, тем граф оказывается более устойчивым, и, соответственно, чем ближе значение τ к 2, тем разрушение такого графа будет происходить быстрее.

Работа выполнена при поддержке Программы стратегического развития на 2012–2016 гг. «Университетский комплекс ПетрГУ в научно-образовательном пространстве Европейского Севера: стратегия инновационного развития».

Литература

1. *Лери М. М.* Моделирование случайных графов Интернет-типа // Обозрение прикладной и промышленной математики. 2009. Т. 16, вып. 5. С. 737–744.

2. *Павлов Ю. Л.* Предельное распределение объема гигантской компоненты в случайном графе Интернет-типа // Дискретная математика. 2007. Т. 19, вып. 3. С. 22–34.

3. *Aiello W., Chung F., Lu L.* A random graph model for massive graphs // Proc. of the 32nd Annual ACM Symposium on Theory of Computing. 2000. P. 171–180.

4. *Bollobas B., Riordan O.* Robustness and vulnerability of scale-free random graphs // Internet Mathematics. 2004. Vol. 1, N 1. P. 1–35.

5. *Cohen R., Erez K., Ben-Avraham D., Havlin S.* Resilience of the Internet to Random Breakdowns // Phys. Rev. Lett. 2000. Vol. 85. P. 4626–4628.

6. *Durrett R.* Random Graph Dynamics. Cambridge: Cambridge Univ. Press, 2007. 212 p.

7. *Faloutsos C., Faloutsos P., Faloutsos M.* On power-law relationships of the internet topology // Computer Communications Rev. 1999. Vol. 29. P. 251–262.

8. *Newman M. E. Y., Strogatz S. H., Watts D. J.* Random graphs with arbitrary degree distribution and their applications // Phys. Rev. E. 2001. Vol. 64. P. 026118.

9. *Matsumoto M., Nishimura T.* Mersenne Twister: A 623-dimensionally equidistributed uniform pseudorandom number generator // ACM Trans. on Modeling and Computer Simulation. 1998. Vol. 8, N 1. P. 3–30.

10. *Norros I., Reittu H.* Attack resistance of power-law random graphs in the finite mean, infinite variance region // Internet Mathematics. 2008. Vol. 5, N 3. P. 251–266.

11. *Reittu H., Norros I.* On the power-law random graph model of massive data networks // Performance Evaluation. 2004. Vol. 55. P. 3–23.

12. *Tangmunarunkit H., Govindan R., Jamin S. et al.* Network topology generators: degree-based vs. structural // Proceedings of the SIGCOMM'02. Pittsburgh, USA, 2002. P. 147–159.

СВЕДЕНИЯ ОБ АВТОРЕ:

Лери Марина Муксумовна
научный сотрудник, к. т. н.
Институт прикладных математических исследований Карельского научного центра РАН
ул. Пушкинская, 11, Петрозаводск, Республика Карелия, Россия, 185910
эл. почта: leri@krc.karelia.ru
тел.: (8142) 781218

Leri, Marina
Institute of Applied Mathematical Research, Karelian Research Centre, Russian Academy of Sciences
11 Pushkinskaya St., 185910 Petrozavodsk, Karelia, Russia
e-mail: leri@krc.karelia.ru
tel.: (8142) 781218