Optimization of Robustness of Complex Networks to Repeated Attacks

T. Tanizawa,[1,2] G. Paul,[1] R. Cohen,[3] S. Havlin,[1,3] and H. E. Stanley[1]

[1] *Center for Polymer Studies and Dept. of Physics, Boston University, Boston, MA 02215, USA*
[2] *Department of Electrical Engineering, Kochi National College of Technology Monobe-Otsu 200-1, Nankoku, Kochi, 783-8508, JAPAN*
[3] *Minerva Center and Department of Physics, Bar Ilan University Ramat Gan 52900, Israel*

We study the robustness of complex random networks to a continuous series of both targeted attacks in which the highest degree nodes are removed and random attacks (or failures) in which nodes are removed randomly. The model is one in which fractions p_t and p_r (representing targeted and random attack, respectively) of the original network are removed repeatedly until the network becomes disconnected. We study networks with scale-free and bimodal degree distributions. We determine the network configuration which maximizes the total fraction of nodes which must be removed before the network collapses. For small values of p_t and p_r, the results depend only on the ratio p_t/p_r. We find that the most robust network degree distribution is bimodal with a fraction r of the nodes having degree $k_2 = (\langle k \rangle - 1 + r)/r$ and the remainder of the nodes having degree 1. The optimal value of r is of the order of p_t/p_r. Even if p_t/p_r is not known, a value of r can be chosen which maximizes the robustness of the network over a wide range of values of p_t/p_r. For large values of $p_t/p_r \simeq 1$ the optimal configuration is one in which all nodes are of degree $\langle k \rangle$.

PACS numbers: 89.20.Hh, 02.50.Cw, 64.60.Ak

Recently, there has been much interest in the resilience of real-world networks to random attacks of nodes or to attacks targeted on the highest degree nodes [1–8]. Many real-world networks are robust to random attack but vulnerable to targeted attack. Given the possibility of terrorist attacks on physical networks and attacks by hackers on computer networks, it is of great importance to understand how to design networks which are as robust as possible against both types of attacks. Studies to date have all treated the case in which there was only one type of attack on a given network – that is, the network was subject to either a random attack or to a targeted attack but not subject to different types of attack in succession. A more realistic scenario is one in which a network is subjected to a continuous series of targeted and random attacks. This scenario can be modeled as a series of alternating targeted and random attacks which remove fractions p_t and p_r of the original nodes, respectively, from the network. The ratio p_t/p_r is kept constant while the individual fractions p_t and p_r approach 0 thus simulating a series of random and targeted attacks which are continuous in time. After some time (after some number m of pairs of random/targeted attacks) the network will become disconnected; at this point a fraction $f = m(p_t+p_r)$ of the nodes will have been removed. We will consider the optimal network design one which maximizes f. We perform our studies under the constraint that the "cost" to construct and maintain a network – defined here to be proportional to the average degree of $\langle k \rangle$ per node in the network – is constant.

We study here two types of networks:

(i) Networks with bimodal degree distributions. In Ref. [8] it was found that under a general metric of robustness, networks with certain specified bimodal degree distributions were optimal to both random attack and targeted attack. We want to determine whether these networks are also optimal to repeated attack.

(ii) Scale free networks. Many real world computer, social, biological and other types of networks have been found to be scale free, i.e., they exhibit degree distributions of the form $P(k) \sim k^{-\lambda}$ [9–17]. For large scale free networks with exponent λ less than 3, it has been found that, if nodes fail randomly, essentially all nodes must fail for the network to become disconnected [3, 4]. On the other hand, because the scale free distribution has a long power-law tail (i.e. hubs with large degree), the networks are vulnerable with respect to targeted attack.

We present arguments that suggest that the degree distribution which optimizes f is a bimodal distribution in which a fraction r of the nodes have degree $k_2 = (\langle k \rangle - 1 + r)/r$ and the remainder of the nodes have degree $k_1 = 1$ and we show that r is of the order of p_t/p_r. Our argument is as follows: To optimize against random removal one wants to maximize the quantity $\kappa \equiv \langle k^2 \rangle / \langle k \rangle$ since for random removal the threshold is determined by [3]

$$f_c^{\rm rand} = 1 - \frac{1}{\kappa - 1}. \qquad (1)$$

Since we keep $\langle k \rangle$ fixed, κ is just the variance of the degree distribution and is maximized with a bimodal distribution in which the lowest degree nodes have the smallest possible degree $k_1 = 1$ and the highest degree nodes have the highest possible degree consistent with keeping $\langle k \rangle$ fixed, $k_2 = (\langle k \rangle - 1 + r)/r$. Thus, k_2 is maximized when r assumes its smallest possible value, $r = 1/N$. On the other hand, if all of the high degree nodes are removed by targeted attacks, the network will be very vulnerable to random attack. So we want to delay as long as possible the situation in which the high degree nodes are removed by the targeted attacks. This argues for not choosing r as small as possible but choosing r such that some high connectivity nodes remain as long as there are some low connectivity nodes. This condition is achieved when r is of the order of(and larger than) p_t/p_r.

Below we we show analytically that this argument is valid for the case in which a single targeted attack followed by a single random attack results in the network becoming disconnected. This is followed by numerical results for the case of many waves of targeted and random attacks; these results support our argument for the optimal configuration.

Single wave of attacks In order to gain insight into the case of repeated random attacks and targeted attacks, we first consider the simpler case of just one set of targeted attacks followed by a set of random attacks.

As described in Ref. [5] targeted attack on a fraction p_t of the most highly connected nodes results in random removal of links from the remaining sites – links that had connected the removed sites with the remaining sites. The probability for a link to lead to a deleted site $\tilde{p}$ equals the ratio of the number of links belonging to the deleted sites to the total number of links. Thus a targeted attack followed by a random attack has the following effect on the degree distribution $P(k)$: (i) the fraction p_t of most highly connected nodes are removed from the distribution, (ii) a fraction $\tilde{p}$ of the remaining sites are randomly removed and, (iii) a fraction p_r of the remaining nodes are removed randomly. Now repeated random attacks which remove fractions $p_{r1}, p_{r2}, \ldots, p_{rk}$ of the nodes are equivalent to a single random attack of a fraction $1-(1-p_{r1})(1-p_{r2})...(1-p_{rk})$ of the nodes. We can use this fact together with Eq. 1 to determine the threshold for the combined random attacks of (ii) and (iii) after the removal in (i) and find

$$1-(1-\frac{p_r}{1-p_t})(1-\tilde{p}) = 1-\frac{1}{\kappa_1 - 1}, \tag{2}$$

where $\kappa_1 \equiv \frac{\langle k^2\rangle_1}{\langle k\rangle_1}$ and where $\langle k\rangle_1$ and $\langle k^2\rangle_1$ are the first and second moments, respectively, of the original distribution with the fraction p_t of the most highly connected nodes removed. Using the fact that $\langle k\rangle_1 = \langle k\rangle - \langle k\rangle\tilde{p}$, we find

$$p_r = 1-(1-p_t)\langle k\rangle \frac{1}{\langle k^2\rangle_1 - \langle k\rangle(1-\tilde{p})}. \tag{3}$$

Since $\langle k\rangle$ and p_t are fixed, we optimize p_r (and therefore $f = p_t + p_r$) when

$$g \equiv \langle k^2\rangle_1 + \langle k\rangle\tilde{p} \tag{4}$$

is maximized. Assume a distribution with n peaks $k_1, k_2, k_3, \ldots, k_n$ with probabilities $r_1, r_2, r_3, \ldots, r_n$, respectively. We want to maximize g subject to the constraints

$$r_1 + r_2 + r_3 + \cdots + r_n = 1, \tag{5}$$
$$r_1 k_1 + r_2 k_2 + r_3 k_3 + \cdots + r_n k_n = \langle k\rangle. \tag{6}$$

This can be accomplished using the method of Lagrange multipliers. We find that the resultant equations obtained by taking derivatives with respect to the r_j are of the form

$$k_j^2 + \lambda_1 + k_j\lambda_2 = 0 \tag{7}$$

where the constants λ_1 and λ_2 are the Lagrange multipliers. Since these equations are quadratic in k_j there are at most 2 unique solutions – establishing the fact that there are at most 2 unique peaks in the distribution which without loss of generality we take as having degrees k_1 and k_2. Solving all the equations we find that

$$k_1 = 1, \tag{8}$$
$$k_2 = k_2^{\text{opt}} = \frac{\langle k\rangle - (1-r)}{r}, \tag{9}$$
$$r_2 = r_{\text{opt}} = \frac{2(\langle k\rangle - 1)p_t}{\langle k\rangle - 1 - p_t}. \tag{10}$$

The maximum value of p_t for which this equation is valid is that for which $r_{\text{opt}} = 1$. At $r = 1$, the optimal solution is that for which $k_1 = k_2 = \langle k\rangle$. Solving Eq. 10 for p_t with $r_{\text{opt}} = 1$ we find the crossover value p_t^* between the two solutions to be

$$p_t^* = \frac{\langle k\rangle - 1}{2\langle k\rangle - 1}. \tag{11}$$

Using Eq. 10, we solve Eq. 2 for p_r and determine $f = p_r + p_t$. In Fig. 4(a), we plot for $\langle k\rangle = 3$ the optimal value of f, f_{opt}, using $k_2 = k_2^{\text{opt}}$ and $r = r_{\text{opt}}$. We also plot f for given values of fixed r.

We perform similar analysis for networks with scale-free degree distributions. However, as shown in Fig. 4(a) the optimal scale free distribution is not as effective as the optimal bimodal distribution and even with r not optimized for a given value of p_t/p_r a value of r can be chosen which still provides better optimization with the bimodal distribution than the optimized scale-free distribution.

Multiple waves of attacks We next study numerically the case in which a small fraction of high-degree nodes, p_t, are removed selectively and repeatedly in a background of uniform random attacks of nodes with the probability, p_r. We show the results for multiple waves of targeted attacks and random attacks against a network with bimodal degree distribution in order to make a comparison with the results for single iteration described in the previous subsubsection.

In Fig. 1, we plot the threshold, f_c of the network with bimodal degree distribution with $\langle k\rangle = 3$ and $r = 10^{-3}$ as a function of the ratio p_t/p_r for various values of p_r. This plot strikingly shows that the values of threshold are essentially independent of the value of p_r itself. We can also see that at $p_t/p_r \sim r$ the threshold reaches the value 0.5 which is the threshold for the single delta function network of $\langle k\rangle = 3$. The fact that the threshold reaches that of the single delta function network of the same $\langle k\rangle$

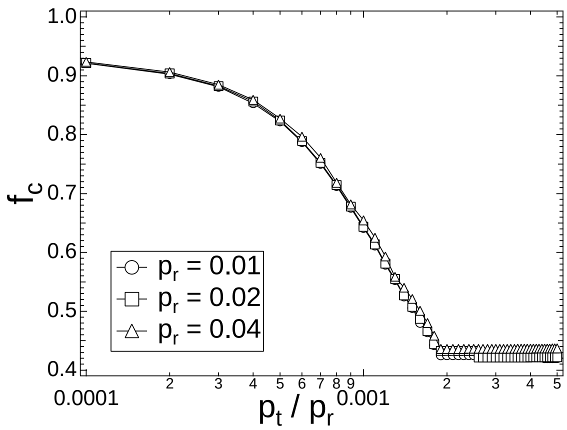

FIG. 1: The plot of the total removal thresholds, f_c of the bimodal network with $\langle k \rangle = 3$ and $r = 10^{-3}$ as a function of the ratio p_t/p_r for various values of p_r. In this plot, the value of k_2 is set to 206 which maximizes the resiliency against one-time attacks. This plot strikingly shows that the values of threshold are independent of the value of p_r itself.

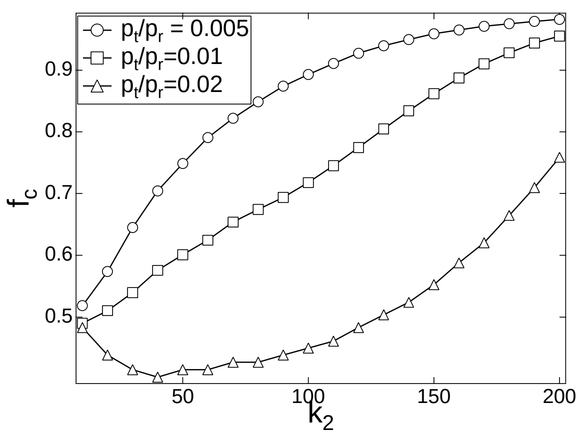

FIG. 2: The thresholds of the bimodal network of $\langle k \rangle = 3$ and $r = 10^{-2}$ for various values of p_t/p_r as a function of k_2. The value of p_r is fixed at 0.02 since the threshold does not depend on p_r explicitly. Notice that the maximum value of k_2 for this case is given by Eq. 9 and equal to 201 in this plot.

at $p_t/p_r \sim r$ for fixed r and k_2 always occurs for any values of the parameters as far as we calculated.

Next we calculate the variation of threshold according to the change of k_2. In the case of single iteration, the maximum value of threshold takes place at the maximum value of k_2 defined by Eq. 9 for a given value of r. The plots are shown in Fig. 2 for the case of $\langle k \rangle = 3$ and $r = 10^{-2}$. From these plots, we can see also in the case of multiple iterations the maximum value of k_2 for each value of p_t/p_r gives the largest values of thresholds.

From the results of our calculation, it is strongly suggested that the ratio $r/(p_t/p_r)$ plays an important role. In Fig. 3, we calculate the maximum values of thresholds for given values of r and p_t/p_r and plot the threshold as a function of the scaled parameter $r/(p_t/p_r)$. Although the values of threshold are different, the behaviors of the curves look very similar. The largest value of each curve occurs at $r/(p_t/p_r) = 1.628$ $(p_t/p_r = 0.005), 1.642$ $(p_t/p_r = 0.01), 1.508$ $(p_t/p_r = 0.02)$. Thus for a given value of the ratio p_t/p_r the optimal value of r, r_{opt} is given by the relation

$$\frac{r_{\text{opt}}}{p_t/p_r} \approx 1.6 \pm 0.06. \tag{12}$$

This relation should be compared to the optimal value of r in the case of single iteration, Eq. 10. When we take $k_2^{\max}$ and r_{opt} according to Eqs. 9 and 10, p_r at the criticality for the single iteration case becomes

$$p_r = 1 - \left(\frac{\langle k \rangle + 1}{\langle k \rangle - 1}\right)^2 p_t + O(p_t^2). \tag{13}$$

Thus for the single iteration case,

$$\frac{r_{\text{opt}}}{p_t/p_r} = 2 - \frac{2\left(\langle k \rangle^2 + \langle k \rangle + 2\right)}{\left(\langle k \rangle - 1\right)^2} p_t + O(p_t^2). \tag{14}$$

Therefore for the single iteration case we have

$$\frac{r_{\text{opt}}}{p_t/p_r} \approx 2. \tag{15}$$

in the region where $p_t \ll 1$. Comparing Eqs. 12 and 15, we might say that multiple iterations cause the change of the value of the optimal ratio, $r_{\text{opt}}/(p_t/p_r)$, from 2 in the case of single iteration to 1.6 in the case of multiple iterations. In the next section, we will obtain a more quantitative evaluation of the value of $r_{\text{opt}}/\left(p_t/p_r\right)$ in the case of multiple iterations.

The smallest value of each curve occurs at $r/(p_t/p_r) = 0.311$ $(p_t/p_r = 0.005), 0.25$ $(p_t/p_r = 0.01), 0.225$ $(p_t/p_r = 0.02)$:

$$\frac{r_{\text{opt}}}{p_t/p_r} \approx 0.26 \pm 0.04. \tag{16}$$

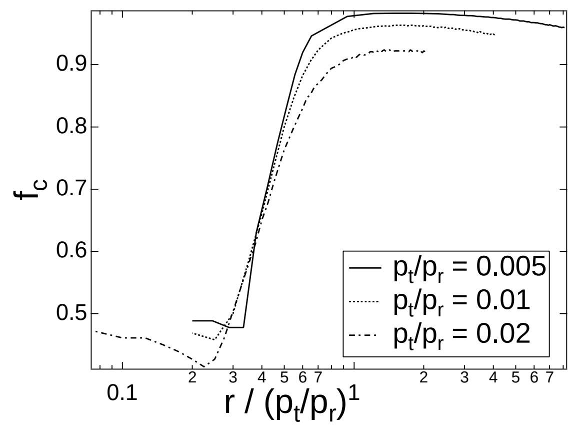

FIG. 3: the optimal values of thresholds in terms of given values of the scaled parameter $r/(p_t/p_r)$. By making plot with respect to this scaled parameter, The curves show similar behavior in their variation.

These values should be compared to $p_t^{\rm crossover}$ in the single iteration case defined by Eq. 11. It is the value of p_t where the probability of targeted attack is too large that the bimodal distribution has no merit. The value of the optimal ratio $r_{\rm opt}/(p_t/p_r)$ in the single iteration case at $p_t^{\rm crossover}$ is

$$\left.\frac{r_{\rm opt}}{p_t/p_r}\right|_{{\rm at}\ p_t^{\rm crossover}} = \frac{\langle k\rangle^2 - 3\langle k\rangle + 1}{(\langle k\rangle - 1)^2}, \tag{17}$$

which takes the value $1/4 = 0.25$ for $\langle k\rangle = 3$.

Discussion and Summary

In Fig. 4, we plot the values of threshold for combination of targeted and random attacks against bimodal networks and scale-free networks in the cases of (a) single iteration and (b) multiple iterations. The optimal values of the ratio r for multiple iterations are numerically determined from the envelope of curves for thresholds of fixed r bimodal distributions:

$$\frac{r_{\rm opt}^{\rm multi}}{p_t/p_r} \approx 1.702 - 5.569\left(\frac{p_t}{p_r}\right) + O\left(\frac{p_t}{p_r}\right)^2. \tag{18}$$

This evaluation should be compare to Eq. 14 for the case of single iteration, which becomes for $\langle k\rangle = 3$

$$\frac{r_{\rm opt}}{p_t/p_r} = 2 - 7p_t + O(p_t^2). \tag{19}$$

The similarity of coefficients is very interesting.

From these plots, we can derive the following conclusions:

- The profiles of these two figures are very similar. Therefore, the analytic results obtained for a single iteration case in the previous section capture most of qualitative features of the resiliency of networks against combined targeted and random attacks quite well.

- Networks of bimodal degree distribution with optimal values of the ratio, r, show very high resiliency against combined attacks with multiple iterations. Though there is no mathematical proof that this type of networks takes the highest values of threshold, we believe so because of the simplicity of the bimodal degree distribution and qualitative argument described in the introduction of this paper.

- Even if we don't know the ratio p_t/p_r in advance, the bimodal networks with $0.03 \lesssim r \lesssim 0.90$ are sufficiently robust for effectively all values of the ratio in the range $p_t/p_r \lesssim 1$. For the attacks with the ratio $p_t/p_r \gtrsim 1$, there is no merit to take heterogeneous degree distributions. In this case, networks with uniform degree distribution are more robust.

- It is very interesting that, while networks for bimodal degree distributions with fixed r and scale-free degree distributions loose their robustness abruptly at certain values of p_t in single iteration cases, those in cases of multiple iterations retain their robustness in wider ranges of the values of the ratio p_t/p_r.

- The difference in the single iteration and the multiple iteration cases can be traced to the fact that the effect of n repeated targeted attacks of the fraction p_t of the nodes of the highest degree is not equivalent to a single targeted attack of the fraction np_t of the nodes of the highest; after each targeted attack, the attacker has information about which of the remaining nodes is the most highly connected and can target them in the next attack. thus many small attacks of strength p_t are more efficient than one attack of strength np_t.

In conclusion, the networks with certain specified bimodal degree distributions are still optimal even if the attacks are repeated combinations of targeted and repeated attacks. In Fig. 5 we show a realization of the type of bimodal network we have discussed here.

We thank L. Braunstein, S. Buldyrev, and S. Sreenivasan for helpful discussions and ONR and Israel Science Foundation for support.

[1] R. Albert, H. Jeong, and A.-L. Barabási, Nature (London) **406**, 378 (2000).

[2] V. Paxon, IEEE/ACM Trans. Networking **5**, 601 (1997).

[3] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, Phys. Rev. Lett. **85**, 4626 (2000).

[4] D. S. Callaway, M. E. J. Newmann, S. H. Strogatz, and D. J. Watts, Phys. Rev. Lett. **85**, 5468 (2000).

[5] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, Phys. Rev. Lett. **86**, 3682 (2001).

[6] R. Cohen, D. ben-Avraham, and S. Havlin, "Structural Properties of scale free networks," Chapter 4 in *Handbook of Graphs and Networks*, edited by S. Bornholdt and H. G. Schuster (Wiley-VCH, New York, 2002).

[7] A. Valente, A. Sarkar, and H. A. Stone, Phys. Rev. Lett. **92**, 118702 (2004).

[8] G. Paul, T. Tanizawa, S. Havlin, and H. E. Stanley, accepted for publication in European Physical Journal B; cond-mat/0404331.

[9] A.-L. Barabási, and R. Albert, Science **286**, 509 (1999).

[10] M. Faloutsos, P. Faloutsos, and C. Faloutsos, Computer Communications Review **29**, 251(1999).

[11] A. -L. Barabási, R. Albert, and H. Jeong, Physica A **281**, 69 (2000).

[12] A. Broder, R. Kumar, F. Maghoul, P. Raghaven, S. Rajogopalan, R. Stata, A. Tomkins, and J. Wiener, Computer Networks **33**, 309 (2000).

[13] H. Ebel, L.-I. Mielsch and S. Bornholdt, Phys. Rev. E. **66**, 128701 (2002).

[14] S. Redner, Eur. Phys. J. B **4**, 131 (1998).
[15] H. Jeong, B. Tombor, R. Albert, Z. N. Oltvai, and A.-L. Barabási, Nature **407**, 651 (2000).
[16] S. N. Dorogovtsev and J. F. F. Mendes, *Evolution of Networks: From Biological Nets to the Internet and WWW* (Oxford University Press, Oxford, 2003).
[17] R. Pastor-Satorras and A. Vespignani, *Evolution and Structure of the Internet: A Statistical Physics Approach* (Cambridge University Press, 2004).
[18] In order to keep $\langle k \rangle$ constant, as we change λ we also must change m, the minimal number of links a node can have. Note that the value of m decreases as we increase λ.
[19] We obtain similar results for other values of $\langle k \rangle$.
[20] P. Erdös and A. Rényi, Publications Mathematicae **6**, 290 (1959).
[21] P. Erdös and A. Rényi, Publications of the Mathematical Inst. of the Hungarian Acad. of Sciences **5**, 17 (1960).
[22] B. Bollabas, *Random Graphs* (Academic, London, 1985).

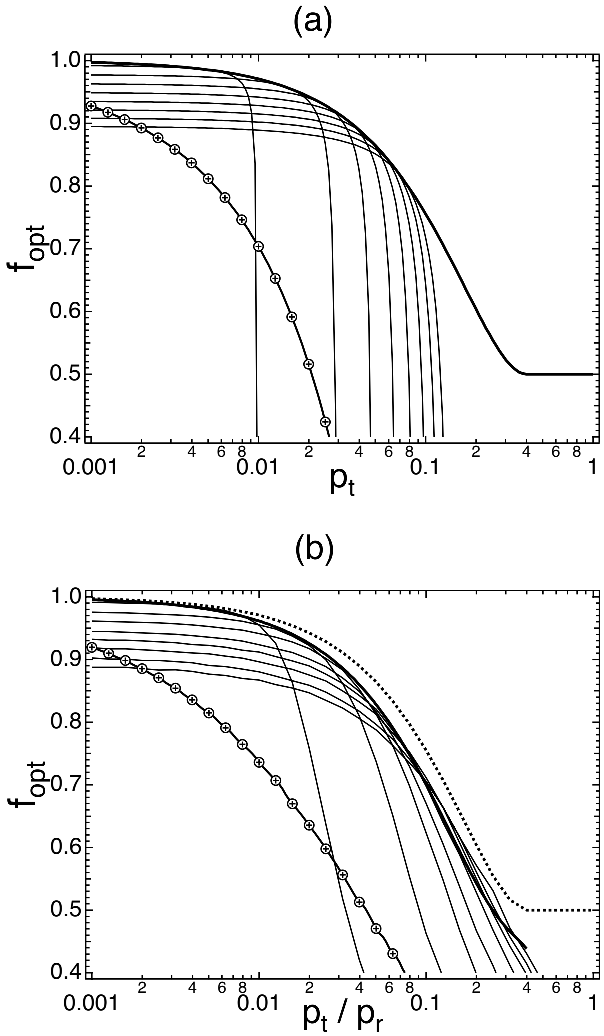

FIG. 4: (a) The optimal values of threshold for single iteration of targeted and random attacks against networks with bimodal degree distribution is plotted with respect to p_t by a solid thick curve. The average value of degree, $\langle k \rangle$ is fixed to be 3. At each value of p_t, the ratio r takes its optimal value determined by Eq. 10. The values of threshold when we fix the ratio r are also plotted in solid thin curves. The values of r are $r = 0.01, 0.03, 0.05, 0.07, 0.09, 0.11, 0.13, 0.15$, respectively from above. For each value of r, k_2 takes its maximum value determined by Eq. 9. We also plot the values of threshold for single iteration of targeted and random attacks against networks with scale-free degree distribution of the exponent $\lambda = 2.3$ and the number of nodes $N = 10000$, which are shown by a solid curve with crossed circle markers ($\oplus$). By increasing the value of λ, the thresholds decrease and approach the value 0.5 which is the threshold for networks with uniform degree distribution of $\langle k \rangle = 3$. From these plots, we can see that the thresholds of bimodal networks with $0.03 \lesssim r \lesssim 0.09$ always dominate over those of scale-free networks. (b) The plots of thresholds for multiple iterations of targeted and random attacks with respect to the ratio p_t/p_r. The description of each curve is the same as that corresponding to the case of single iteration. We also add the optimal values of threshold for single iteration by a dotted curve for comparison. As in the case of single iteration, the thresholds of bimodal networks with $0.03 \lesssim r \lesssim 0.09$ still dominate over those of scale-free networks also in the case of multiple iteratons.

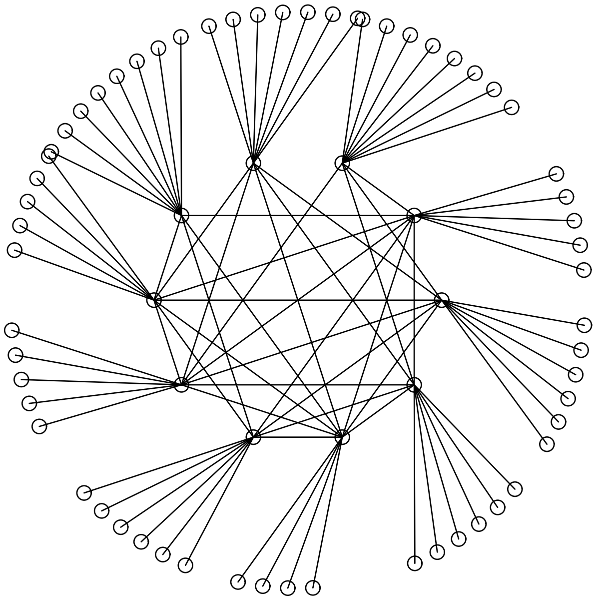

FIG. 5: Realization of bimodal network with $N = 100$, $\langle k \rangle = 2.1$ and $r = 0.1$