Developing Analytical Framework to Measure Robustness of Peer-to-Peer Networks

Bivas Mitra, Md. Moin Afaque, Sujoy Ghose, Niloy Ganguly

Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur, India
{bivasm,moin,sujoy,niloy}@cse.iitkgp.ernet.in

Abstract. In peer-to-peer (p2p) networks, peer nodes communicate with each other with the help of overlay structure. As the peers in the p2p system join and leave the network randomly, it makes the overlay network dynamic and unstable in nature. In this paper, we propose *an analytical framework* to assess the robustness of different topologies adopted by these overlay structures, to withstand the random movement of peers in the networks. We model the dynamic behavior of the peers through degree independent as well as degree dependent node failure. Recently superpeer networks are becoming the most widely used topology among the p2p networks [8]. Therefore we perform the stability analysis of superpeer networks as a case study. We validate the analytically derived results with the help of simulation.

Key words: peer to peer networks, complex networks, percolation theory, network resilience

1 Introduction

Peer to peer (p2p) networks have recently become a popular medium through which huge amount of data can be shared. P2p file sharing systems, where files are searched and downloaded among peers without the help of central servers, have emerged as a major component of Internet traffic. Peers in p2p networks are connected among themselves by some logical links forming an overlay above the physical network. It has been found that these overlay networks, consisting of a large amount of peers are analogous to complex real world networks and can be modeled using various types of random graphs [15]. Generally the degrees of these random graphs are statistically distributed and become the characteristic feature of the topology of the overlay networks.
The topology of the overlay network is important from two aspects.

- The spread of information flow through the network is essential to perform efficient search in the p2p networks. The speed at which information spread is dependent on the topology of the network.

- As peers in the p2p system join and leave network randomly without any central coordination, overlay structures become highly dynamic in nature.

Frequently it partitions the network into smaller fragments which results in the breakdown of communication among peers.

In this paper we concentrate on understanding the stability[1] of the overlay structures which is a major challenge in front of the p2p network community. There is no formal framework available to measure the stability of various overlay structures modeled by random graphs. However different works in bits and pieces have been done mainly by the physicists which analyzes the dynamics of random graphs. Effect of random failures and intentional attacks in various kind of graphs are discussed by Cohen *et al.* in [1, 2]. It has been observed from the results that Internet, which can be modeled by power law networks is more resilient to random failure than E-R graphs (Poisson random graphs). They also found both analytically and experimentally that scale free networks are highly sensitive to intentional attack leading support to the view of Albert [3]. In [4], Newman *et al.* developed the theory of random graphs with arbitrary degree distribution with the help of generating function formalism. Using this formalism, Callaway [5] found the exact analytic solutions for percolation[2] on random graphs with any degree distribution where failure has been modeled by an arbitrary function of node degree. In [7], researchers have addressed a more realistic scenario in which a network is subjected to simultaneous targeted and random attacks. This attack has been modeled as a sequence of "waves" of targeted and random attacks which removes fractions p_t and p_r of the nodes of the network. In all these works except [5], researchers have considered some particular types of networks like E-R, scale free or bimodal networks and analyzed the effect of a few specific kinds of failures like random, intentional or mixed upon them. In [5], researchers have dealt a more general case but failed to propose any generalized equation to measure the stability of random graphs. This paper utilizes many of aforesaid results and proposes a generalized equation to measure stability of p2p overlay structures against dynamic movement of peers.
As examples of random and frequent movement of peers, we model two kinds of node failures in random graph.

- The most common type of failures are denoted as *degree independent failure* where probability of removal of a node is constant and independent of degree of that node.
- In p2p networks, peers having higher connectivity (e.g. superpeers) are more stable in the network than the peers having lower connectivity because those loosely connected peers enter and leave the network quite frequently. These observation leads us to model a new kind of failure where probability of removal of a node is inversely proportional to the degree of that node. We denote this kind of failure as *degree dependent failure*.

[1] In this paper, we do not differentiate between the terms stability and robustness. They are therefore used interchangeably.

[2] Percolation indicates the existence of a critical probability p_c such that below p_c the network is composed of isolated clusters but above p_c, a giant cluster spans the entire network.

As example of topology, we consider superpeer networks. This is because, as most widely used overlay structures, considerable amount of interest has been recently generated in understanding the stability of these networks. We also verify the correctness of our theoretical model with the help of experimental results.
The rest of the paper is organized as follows. Section 2 models the generalized random graph for any kind of failures. It shows the condition for giant component disruption for any kind of disturbances in the networks. In section 3 we classify two different kinds of random failure and mathematically analyze their effect on the generalized random graph. Section 4 theoretically examines the stability of superpeer networks for degree independent and degree dependent failures. This section also compares the results derived from our mathematical model with experimental results. Section 5 concludes the paper.

2 Stability analysis of overlay networks

In this section, we use generating function formalism to derive the general formula for measuring the stability of overlay structures undergoing failure. We formally model the overlay structures and various kinds of failures and define the stability metric which are the parameters of our analytical framework.

2.1 Topology of the overlay networks

The different types of overlay structure of the p2p networks can be modeled using the uniform framework of probability distribution p_k, where p_k be the probability that a randomly chosen node has degree k. So the degree distribution p_k signifies the topology of the overlay network which can be modeled as E-R graph, power law network, superpeer network or any other arbitrary topology. The most common overlay structures are the simple unstructured p2p networks where data are shared among peers in a naive fashion. In such a system like Gnutella [12], all peers have equal roles and responsibilities. Such topologies can be modeled by E-R graph with degree distribution $p_k = \frac{z^k e^{-z}}{k!}$ where z is the mean degree or power law network $p_k = ck^{-\beta}$ where β is a parameter and c is a constant.
Recently, the superpeer networks have become a potential candidate to model overlay structure where a small fraction of nodes are superpeers and rest are peers. Many popular p2p systems like KaZaA [13] have adopted superpeers in their design. A superpeer node having higher connectivity, acts as a centralized server to a subset of clients where client peers submit queries to their superpeer and receive results from it. However superpeers are also connected to each other to route messages over the overlay network and submit and answer queries on behalf of their clients and themselves. Superpeer networks can be modeled by bimodal degree distribution where a large fraction (r) of peer nodes with small degree k_l are connected with superpeers and few superpeer nodes ($1 - r$) with high degree k_m are connected to each other. Formally

$$p_k > 0 \quad if \;\; k = k_l, k_m; \qquad p_k = 0 \quad otherwise$$

k_l & k_m are degrees of peers and superpeers respectively.

2.2 Different kinds of failure models

Let q_k be the probability that a vertex of degree k be present in the network after the removal of a fraction of nodes. In our framework q_k is used to specify the various failure models.

- In degree independent random failure, the probability of removal of any randomly chosen node is constant, degree independent and equal for all other nodes in the graph. Therefore the presence of any randomly chosen node having degree k after this kind of failure is $q_k = q$ (independent of k).

- In degree dependent random failure, probability of failure of a node (f_k) having degree k is inversely proportional to k^γ. i.e $f_k \propto 1/k^\gamma \Rightarrow f_k = \alpha/k^\gamma$ where $0 \leq \alpha \leq 1$ and γ is a real number. Therefore probability of the presence of a node having degree k after this kind of failure is $q_k = (1 - \frac{\alpha}{k^\gamma})$.

2.3 Stability metric

The stability and robustness of overlay networks are primarily measured in terms of certain fraction of nodes f_c called percolation threshold or critical fraction [10], removal of which disintegrates the network into smaller, disconnected components. Below that threshold, their exists a connected component which spans the entire network also termed as giant component[3]. The value of percolation threshold or critical fraction f_c signifies the stability of the network, higher value indicates greater stability against failure.

2.4 Generating function formalism

Based upon the above described model parameters, we use generating function formalism to find out the general formula to measure the stability of various overlay structures. In mathematics a generating function is a formal power series whose coefficients encode information about a sequence that is indexed by the natural numbers [4]. This generating function can be used to understand different properties of graphs. For example, the generating function $G_0(x)$ generates the probability distribution of the vertex degrees k. Therefore $G_0(x) = \sum_{k=0}^{\infty} p_k x^k$ where p_k is the probability that a randomly chosen vertex in the graph has degree k. Importance of the generating function lies in the convenient way the average over the probability distribution can be generated - for instance, the average degree z of a vertex in the case of $G_0(x)$ is given by $z = \langle k \rangle = \sum_k k p_k = G_0'(1)$. Higher moments can be calculated from higher derivatives also. Here we are using the generating function to explain a slightly more complicated concept.

[3] Giant component is a technical term which signifies the largest connected component in the network whose size is of the order of size of the network [11].

In our formalism q_k and p_k specifies the failure model and network topology respectively whose stability is subjected to examination. The formalism helps us to locate the transition point where the giant component breaks down into smaller components. $p_k.q_k$ specifies the probability of a node having degree k to be present in the network after the process of removal of some portion of nodes is completed. Hence

$$F_0(x) = \sum_{k=0}^{\infty} p_k.q_k x^k$$

becomes the generating function for this distribution. Distribution of the outgoing edges of the first neighbor of a randomly chosen node can be generated by

$$F_1(x) = \frac{\sum_k k p_k q_k x^{k-1}}{\sum_k k p_k} = F_0'(x)/z$$

where z is the average degree [5].

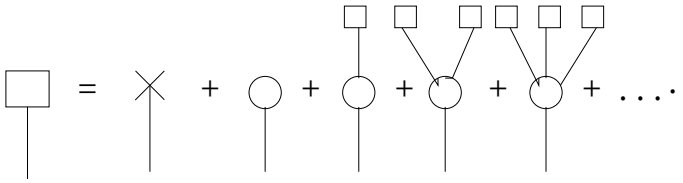


Fig. 1. Schematic representation of the sum rule for the connected component of vertices reached by following a randomly chosen edge. The probability of each such component (left-hand side) can be represented as the sum of the probabilities (right hand side) of having no vertex (which has been removed), only a single vertex, having a single vertex connected to one other component, or two other components, and so forth. The entire sum can be expressed in closed form as equation (1) and similarly (2).

Let $H_1(x)$ be the generating function for the distribution of the component sizes that are reached by choosing a random edge and following it to one of its ends. The component may contain zero node if the node at the other end of the randomly selected edge is removed, which happens with probability $1-F_1(1)$, or the edge may lead to a node with k other edges leading out of it other than the edge we came in along, distributed according to $F_1(x)$. That means that $H_1(x)$ satisfies a self-consistency condition (Fig. 1) of the form [5]

$$H_1(x) = 1 - F_1(1) + xF_1(H_1(x)). \tag{1}$$

The distribution for the component size to which a randomly selected node belongs to is similarly generated by (Fig. 1) $H_0(x)$ where

$$H_0(x) = 1 - F_0(1) + xF_0(H_1(x)). \tag{2}$$

Therefore the average size of the components becomes

$$H_0'(1) = \langle s \rangle = F_0(1) + \frac{F_0'(1)F_1(1)}{1 - F_1'(1)}$$

which diverges when $1 - F_1'(1) = 0$. Size of the component becoming infinite implies that the entire network joins together forming one giant component.

$$F_1'(1) = 1 \Rightarrow \sum_{k=0}^{\infty} kp_k(kq_k - q_k - 1) = 0 \tag{3}$$

The equation (3) states the critical condition for the stability of giant component with respect to any type of graphs (characterized by p_k) undergoing any type of failure (characterized by q_k). Formulating this general formula is the primary contribution of the paper. In the rest of the paper, we investigate the stability situation under various special conditions.

3 Stability at various failure scenario

We have seen that random movement of the peers in the p2p network can be modeled by different kinds of failures in the complex graph. As discussed, we address two kinds of random failures - degree independent and degree dependent. In the next two subsections, we deal with these two kinds of failures and investigate their effect on the stability of overlay structure modeled by generalized random graph.

3.1 Degree independent random failure

In this section, we discuss the effect of degree independent random failure in generalized random graph. If $q = q_c$ is the critical fraction of nodes whose presence in the graph is essential for the stability of the giant component after this kind of failure then according to equation (3)

$$\sum_{k=0}^{\infty} kp_k(kq_c - q_c - 1) = 0$$

$$\Rightarrow q_c = \frac{1}{\frac{\langle k^2 \rangle}{\langle k \rangle} - 1}$$

Now if f_c is the critical fraction of nodes whose random removal disintegrates the giant component then $f_c = 1 - q_c$. Therefore percolation threshold

$$f_c = 1 - \frac{1}{\frac{\langle k^2 \rangle}{\langle k \rangle} - 1} \tag{4}$$

This is the well known condition [1] (derived differently) for the disappearance of the giant component due to random failure. Note that, we have reproduced it to show that it can also be derived from the proposed general formula (equation 3).

3.2 Degree dependent random failure

In p2p networks, the peers (or superpeers) having higher connectivity are much more stable and reliable than the nodes having lower connectivity. Therefore probability of the presence of a node having degree k after this kind of failure is

$$q_k = (1 - \frac{\alpha}{k^\gamma}). \tag{5}$$

Using equations (3) and (5), we obtain the following critical condition for the stability of giant component after degree dependent breakdown

$$\langle k^2 \rangle - \alpha \langle k^{2-\gamma} \rangle + \alpha \langle k^{1-\gamma} \rangle - 2\langle k \rangle = 0$$

where percolation threshold is

$$f_c = \sum_{k=0}^{\infty} \frac{\alpha}{k^\gamma} p_k.$$

Considering the value of $\alpha = 1$, where the fraction of nodes removed due to this kind of failure becomes maximum, the condition for percolation becomes

$$\langle k^{2-\gamma} \rangle - \langle k^{1-\gamma} \rangle = \langle k^2 \rangle - 2\langle k \rangle \tag{6}$$

Thus the critical fraction of nodes removed is given by

$$f_c = \sum_{k=0}^{\infty} \frac{1}{k^\gamma} p_k. \tag{7}$$

where γ satisfies the equation (6).

Thus from the equations (6) and (7), we can determine the variation of percolation threshold f_c for various networks due to degree dependent random failure. We apply these formalism for superpeer networks and compare the results with experimental results in section 4.

4 Case study: Stability of superpeer networks with respect to failure models

In this section we study the robustness of the superpeer networks with the help of our analytical framework. We investigate the change of percolation threshold (f_c) due to the change of fraction of peers (r) and the connectivity of the superpeers (k_m) in the networks for various types of failure. To ensure fair comparisons, we keep *the average degree* $\langle k \rangle$ *constant for all graphs*. We verify our theoretical results with the help of experiments; the experimental setup is explained below.

4.1 Experimental setup

The p2p overlay structure is represented by a simple undirected graph stored as an adjacency list. In order to generate the topology, every node is assigned a degree according to the topology being simulated. In the case of bimodal network the nodes are assigned the degrees depending on the k_l and k_m values and the fraction of these nodes in total. Thereafter the edges are generated using the "switching method" and the "matching method" referred to in [14]. However since these methods (as far as our knowledge goes, no better method exists) do not sample the total ensemble of all possible desired graphs (here bimodal) uniformly, the experimental results might vary a little from the theoretical results. Failure of a peer effectively means deletion of the node and its corresponding edges. In the case of degree independent failure, nodes are randomly selected using a time-seeded pseudo-random number generator and its edges removed from the adjacency list. In degree dependent failure, first the fraction of nodes having a certain degree that need to be removed is calculated, thereafter that many nodes are selected from the total set of all such nodes randomly and its corresponding edges are removed from the adjacency list.

4.2 Degree independent failure

Bimodal structure is mostly used to model superpeer networks. Let r be the fraction of peers in the superpeer networks having degree k_l and and rest are superpeers having degree k_m where $k_l << k_m$. Therefore bimodal degree distribution p_k becomes non zero only at k_l and k_m [6]. Mathematically

$k_l p_{k_l} + k_m p_{k_m} = \langle k \rangle$ and $p_{k_l} + p_{k_m} = 1$ which provides

$$p_{k_m} = \frac{\langle k \rangle - k_l}{k_m - k_l} \qquad\qquad p_{k_l} = \frac{k_m - \langle k \rangle}{k_m - k_l}$$

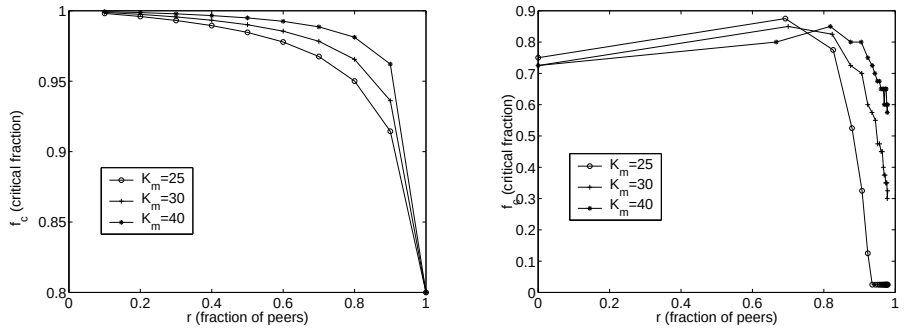
$\Rightarrow \langle k^2 \rangle = k_m^2 p_{k_m} + k_l^2 p_{k_l} = \langle k \rangle (k_l + k_m) - k_l k_m$ and using equation (4) we get

$$f_c = 1 - \frac{\langle k \rangle}{\langle k \rangle (k_l + k_m - 1) - k_l k_m}$$

As the fraction of peers having degree k_l in the network is r therefore the average degree of the network $\langle k \rangle = k_l r + k_m (1 - r)$ implies that $k_l = \frac{\langle k \rangle - (1-r)k_m}{r}$. Hence percolation threshold

$$f_c = 1 - \frac{\langle k \rangle r}{\langle k \rangle^2 - 2\langle k \rangle k_m + 2 r k_m \langle k \rangle - r \langle k \rangle + k_m^2 - r k_m^2} \tag{8}$$

Using equation (8), we study the variation of percolation threshold (f_c) due to the change of the fraction of peers (r)(Fig 2(a)). Here we keep the average degree $\langle k \rangle = 5$ fixed and vary the superpeer degree $k_m = 25, 30, 40$ for each curve. The results for the same parameters are also deduced experimentally and shown in Fig 2(b). We first explain the features commonly observed in both theoretical



(a) Theoretical (b) Experimental

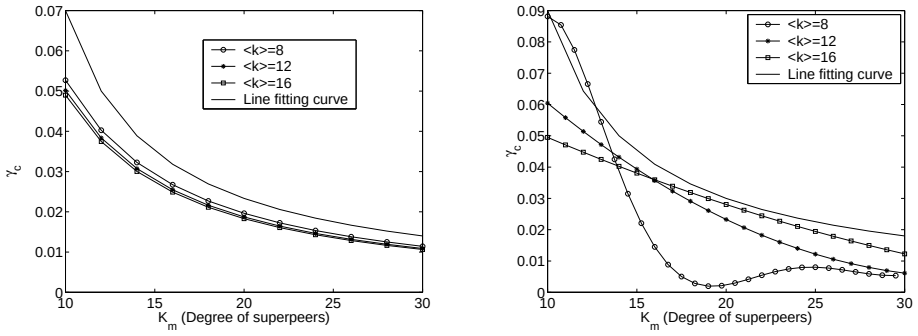
Fig. 2. The above plots represent critical fraction (f_c) Vs fraction of peers (r) for various superpeer networks undergoing degree independent failure. Here X-axis represents the fraction of peer nodes (r) exists in the superpeer network and Y-axis represents the corresponding critical fraction or percolation threshold (f_c).

and practical results and then provide a comparative study between the two results.

General observations: It can be observed (in both theoretical and experimental results) that with the increase of the fraction of peers in the network, the percolation threshold decreases which indicates the increase of fragility of the network. That means increase of the fraction of superpeers in the network improves the stability of the network. When the fraction of superpeers is above 15% to 20% , the percolation threshold is quite high. But after that, there is a sharp fall of f_c thus drastically increases the vulnerability of the network.

Comparative study between theoretical and experimental results: It can be observed from the theoretical (Fig.2(a)) and experimental (Fig.2(b)) results that the behavior of critical fraction (f_c) with the change of the percentage of peers (r) is almost same for both cases. The only significant observation for the experimental result is when percentage of superpeers is quite high (80% to 90%), the value of f_c starts from a lower value. With the decrease of superpeers fraction, f_c goes up and reaches an optimum value. This indicates the optimum superpeer to peer ratio for which overlay network becomes most stable due to this kind of failure. The further decrease of superpeers again reduces the value of f_c. The initial increase of f_c cannot be captured by our analytical model. From the theoretical perspective, giant component size is the order of the network size and is intuitively considered same for all cases. But in practice, giant component is a finite fraction of size of the network which is not fixed for all cases but may vary (albeit slightly) from case to case. For the lower values of r (i.e. percentage of superpeers is high), some superpeers remain isolated in the network thus

reducing the size of the giant component. This results in lower values of f_c. But with the decrease of percentage of superpeers, all the superpeers get connected which increases the stability of the network.



(a) Theoretical (b) Experimental

Fig. 3. Change of γ_c with respect of superpeer degree k_m for superpeer networks undergoing degree dependent failure. Here mean degree $\langle k \rangle$ varies from 8 to 16. X-axis represents the superpeer degree(k_m) and Y-axis represents the corresponding γ_c.

4.3 Degree dependent failure

As introduced in section 2, in this case the probability of failure of a node is inversely proportional to the degree of that node. Mathematically the fraction of nodes removed $f = \sum_{k=0}^{\infty} \frac{\alpha}{k^{\gamma}} p_k$. According to equation (6), the bimodal network percolates if

$$\langle k^{2-\gamma} \rangle - \langle k^{1-\gamma} \rangle = \langle k^2 \rangle - 2\langle k \rangle.$$

If the value of $\gamma = \gamma_c$ satisfies this equation then removal of $f_c = \sum_{k=0}^{\infty} \frac{1}{k^{\gamma_c}} p_k$ fraction of nodes destroys the giant component. In most of the commercial superpeer networks like KaZaA [13], peers are only directly connected to the local superpeer making their degree $k_l = 1$. In that case, the value of γ_c which percolates the bimodal network can be derived from equation (6) and becomes

$$\gamma_c = 1 - \frac{\ln \frac{\langle k \rangle (k_m + 1) - k_m - 2\langle k \rangle}{\langle k \rangle - 1}}{\ln k_m} \tag{9}$$

where lowest degree is assumed to be $k_l = 1$. We plot the variation of the γ_c that is required to percolate the bimodal networks with respect to the superpeer degree k_m for various average degree $\langle k \rangle$(Fig 3(a)). Like degree independent failure, the results for the same parameters are also deduced experimentally and

shown in Fig 3(b). We first explain the features commonly observed in both theoretical and practical results and then provide a comparative study between the two results.

General observations: It can be easily identified from Fig 3, that with the increase of superpeer degree, the value of γ_c that percolates the network decreases. These curves can be approximated by the polynomial $a/(x-b)$ ($0 < a < 1$ and b is some positive integer). Thus the decrease of γ_c follows hyperbolic trajectory. Another interesting observation is after a certain threshold k_m, the curves become parallel to the X-axis and never cuts it thus the value of γ_c is small but never becomes 0 (in that case $f_c = \sum_{k=0}^{\infty} \frac{1}{k^0} p_k = 1$). It implies that for any large value of k_m, although f_c becomes significantly large however it is required to remove only a part of nodes (and not all the nodes) from the network to dissolve the giant component.

Comparative study between theoretical and experimental results: In the case of degree dependent failure, the experimental results (Fig.3(b)) differ from theoretical (Fig.3(a)) for lower average degree $\langle k \rangle$ but matches quite well for higher values of $\langle k \rangle$. In both cases, initially γ_c decreases with the increase of superpeer degree (k_m). But after crossing a threshold value (which also reflects the optimum superpeer degree), further increases of k_m increases the value of γ_c which is not reflected by the theoretical analysis. The reason is almost same as explained in degree independent failure. Keeping average degree constant and increasing the superpeer degree leaves many of the superpeers isolated. This decreases the stability of the network thus increases the value of γ_c. This phenomenon becomes significant when the average degree of the network is low.

5 Conclusion and future work

The basic contribution of this work is the development of general framework to analyze the stability of various p2p overlay structures against dynamic movement of peers. We have modeled the behavior of these peers using degree independent and degree dependent random failure. As superpeer networks are currently most promising and widely used overlay structure, we perform stability analysis of these networks as a case study of our analytical model. It has been observed that when the fraction of superpeers in the network is less than 15%, the robustness of the network sharply decreases for degree independent failure. This result points to a zone where superpeer network is most vulnerable. Similarly for degree dependent failure, our analysis shows that increase of superpeer degree improves the stability of the network and the improvement follows a hyperbolic trajectory. Although our theoretical and experimental results have matched fairly, however the little differences between them result from the contradiction of the theoretical and practical concept of giant component. Difficulties to generate accurate graph with a given degree sequence are also responsible for the slight mismatch between theoretical and experimental results.

Deeper look into the differences between experimental and theoretical results is part of our future work. Similarly we have to perform a detailed compara-

tive study of the stability of various overlay topologies like E-R graph, power law network, various kinds of superpeer networks like mixed Poisson and bimodal structure etc. In addition to the simple failure models discussed here, in future we will consider different kinds of attacks where nodes having more importance are been targeted and attacked to destroy the connectivity of the p2p network. Importance of a node can be determined by degree centrality, betweenness, eigenvector centrality etc. Moreover, comparative stability analysis of all these topologies with respect to combination of different attacks and failures will bring completeness to the work.

References

1. R. Cohen, K. Erez, D. Avraham, S. Havlin : "Resilience of the Internet to Random Breakdown", Vol. 85, No. 21 Physical Review Letters, 2000.
2. R. Cohen, K. Erez, D. Avraham, S. Havlin : "Resilience of the Internet under Intentional Attack", Vol. 86, No. 16 Physical Review Letters, 2001.
3. R. Albert, H. Jhong, A. L. Barabsi : "Error and Attack Tolerance of Complex Networks", Nature, 406, 2000.
4. M. E. J. Newman, S. H. Strogatz, D. J. Watts : "Random Graphs with Arbitrary Degree Distributions and Their Application", Physical Review , 2001.
5. D. S. Callaway , M. E. J. Newman, S. H. Strogatz, D. J. Watts : "Network Robustness and Fragility: Percolation on Random graphs", Vol. 85, No. 21 Physical Review Letters, 2000.
6. G. Paul, Sameet Sreenivasan, Shlomo Havlin, Stanley : "Resilience of the Internet to Random Breakdown", Phys Rev E, 72, 056130, 2005.
7. T. Tanizawa, G. Paul, R. Cohen, S. Havlin, H.E. Stanley : "Optimization of Network Robustness to Waves of Targeted and Random Attack", Physical Review E.,71,047101, 2005.
8. B. Yang, H. Garcua-Molina : "Designing a Super-Peer Networks ", Proceedings of the International Conference on Data Engineering (ICDE), Los Alamitos, CA, March 2003.
9. A. Valente, A. Sarkar, H. A. Stone : "2-Peak and 3-Peak Optimal Complex Networks", Physical Review Letters, 92: 118702, 2004.
10. M. Molloy, B. Reed : "A Critical Point for Random Graphs with a Given Degree Sequence", Random Structures and Algorithms 6, 161-179, 1995.
11. M. Molloy, B. Reed : "The Size of the Giant Component of a Random Graph with a Given Degree Sequence", Combinatorics, Probability and Computing 7, 295-298, 1998.
12. Gnutella website. http://www.gnutella.com
13. KaZaA website. http://www.kazaa.com
14. R. Milo, N. Kashtan, S. Itzkovitz, M. E. J. Newman, U. Alon : "On the Uniform Generation of Random Graphs with Prescribed Degree Sequences", eprint arXiv:cond-mat/0312028, 2003.
15. Q. Lv, P. Cao, E. Cohen, K. Li and S. Shenker : "Search and Replication in Unstructured Peer-to-Peer Networks", ACM International Conference on Supercomputing, New York, USA, 2002.