Brief Announcement: Measuring Robustness of Superpeer Topologies

B. Mitra
Dept. of CSE
IIT Kharagpur, India
bivasm@cse.iitkgp.ernet.in

F. Peruani
ZIH, Technical University of Dresden, Germany
peruani@mpipks-dresden.mpg.de

S. Ghose, N. Ganguly
Dept. of CSE
IIT Kharagpur, India
{sujoy, niloy}@cse.iitkgp.ernet.in

Categories and Subject Descriptors: C.4 [PERFORMANCE OF SYSTEMS]: Modeling techniques

General Terms: Performance

Keywords: Superpeer networks, stability, percolation theory

1. INTRODUCTION

Peers in the superpeer system join and leave the network randomly without any central coordination. This churn of nodes might partition the network into smaller fragments and breakdown communication among peers. But in practice, superpeer overlay networks exhibit stable behavior against churn. However the stability of the overlay network can get severely affected through intended attacks targeted towards the important peers [1]. In this paper, we propose *an analytical framework* using percolation theory to assess the robustness of superpeer topologies in face of churn and attack. The main contribution of the paper lies in developing a quantitative measure to analyze the stability of the networks against all these dynamics. The results obtained from the theoretical analysis are validated through simulation.

2. ANALYTICAL FRAMEWORK

In this section, we use generating function to derive the general formula for measuring the stability[1] of overlay structures undergoing any kind of disturbances in the network. We explain the basic concept behind development of the framework without going into mathematical details. Let p_k be the probability of finding a node with degree k chosen uniformly at random and q_k be the probability that a node of degree k survives the failure or attack. We are going to establish the relationship between stability and p_k and q_k using the generating function formalism. $p_k.q_k$ is 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. Following the derivation explained in [2], we find the average size of the components

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

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.

$$F_1'(1) = 1 \Rightarrow \sum_{k=0}^{\infty} k p_k (k q_k - q_k - 1) = 0 \qquad (1)$$

The Eq. (1) states the critical condition for the formation of giant component for any type of graphs (characterized by p_k) undergoing any type of disrupting event (characterized by $1 - q_k$).

3. ENVIRONMENTAL DEFINITION

Topology of the overlay networks can be modeled using the uniform framework of degree distribution p_k. In this paper, we model superpeer networks by using bimodal degree distribution. In bimodal network, a large fraction (r) of peer nodes have small degree k_l while a few superpeer nodes ($1 - r$) have high degree k_m. Formally

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

Churn and attack models are specified through the model parameter q_k.

1. In churn, the probability of removal of any randomly chosen node is degree independent and equal (constant) 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).
2. In targeted attack, the nodes having high degrees are progressively removed. Formally

$q_k = 0$ when $k > k_m$

$0 \leq q_k < 1$ when $k = k_m$

$q_k = 1$ when $k < k_m$.

This removes a fraction of nodes from the network with degree $\geq k_m$.

Stability metric: The stability of overlay networks are measured in terms of percolation threshold f_c. f_c signifies a critical fraction of the nodes, removal of which disintegrates the network. The percolation threshold is measured

[1]In this paper, we do not differentiate between the terms stability and robustness.

PODC'07, August 12–15, 2007, Portland, Oregon, USA.
ACM 978-1-59593-616-5/07/0008.

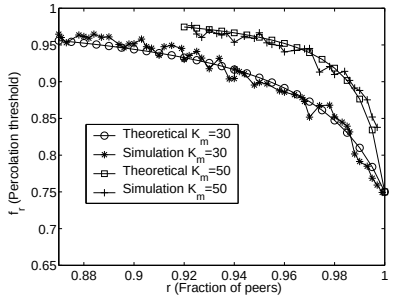

Figure 1: The above plots represent a comparative study of theoretical and simulation results of stability for two bimodal networks undergoing churn. We keep the average degree $\langle k \rangle = 5$ fixed and vary the superpeer degree $k_m = 30, 50$ for two plots.

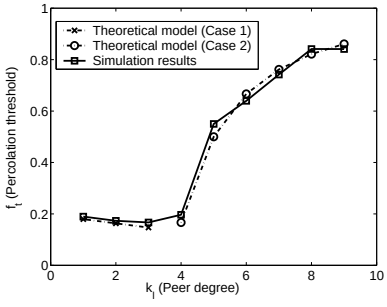

Figure 2: The above plot shows the behavior of the bimodal network in face of targeted attack found experimentally and compares it with the proposed theoretical model. We keep the average degree $\langle k \rangle = 10$ and superpeer degree $k_m = 50$ fixed.

experimentally in the following way. During simulation, we remove a fraction of nodes from the network in each step. After each step t, we find out the status of the network in terms of component size distribution $CS_t(s) = sn_s / \sum_s sn_s$ where s and n_s respectively are the size of the component formed and the number of components of size s. The component size distribution initially exhibits unimodal characteristics. Eventually at a particular step $t = t_n$, $CS_t(s)$ becomes monotonically decreasing function indicating t_n as percolation point and the total fraction of nodes removed upto this point specifies percolation threshold.

4. STABILITY OF SUPERPEER NETWORKS

Effect of churn

The superpeer networks mostly suffer from the churn of peers which can be modeled by the random failure of nodes in complex graph. We use our equation to show that stability of the superpeer networks is quite unaffected due to churn of peers. The critical fraction f_r required to be removed to disintegrate a general network can be obtained from Eq. (1)

$$f_r = 1 - \frac{1}{\langle k^2 \rangle / \langle k \rangle - 1} \tag{2}$$

where $\langle k \rangle$ and $\langle k^2 \rangle$ are the first and second moment of the degree distribution respectively. The customized equation for bimodal network becomes

$$f_r = 1 - \frac{\langle k \rangle r}{\langle k \rangle^2 - 2\langle k \rangle k_m + 2rk_m\langle k \rangle - r\langle k \rangle + k_m^2 - rk_m^2} \tag{3}$$

Observations:

1. It is important to observe (Fig. 1) that for the entire range of peer fractions r, the percolation threshold f_r is greater than 0.7 which implies that superpeer networks are quite robust against churn.
2. Another significant observation is, lower fraction of superpeers in the network (specifically when it is below 5%) results in a sharp fall of f_r (Fig. 1).

Effect of attack

Stability of the superpeer networks is challenged by progressively attacking the prominent superpeers and peers. Two cases may arise

Case 1 : Removal of a fraction of superpeers is sufficient to disintegrate the network. The percolation threshold f_t for case 1 can be obtained from Eq. (1)

$$f_t = (1 - r)\left(1 - \frac{\langle k \rangle - k_l(k_l - 1)r}{k_m(k_m - 1)(1 - r)}\right) \tag{4}$$

Case 2: Removal of all the superpeers is not sufficient to disintegrate the network. Therefore we need to remove some of the peer nodes along with the superpeers. The percolation threshold for case 2 becomes

$$f_t = r\left(1 - \frac{\langle k \rangle}{k_l(k_l - 1)r}\right) + (1 - r) \tag{5}$$

Observations:

1. In the networks with peer degree $k_l = 1, 2$ and 3, the removal of only a fraction of superpeers causes breakdown hence makes these networks vulnerable (Fig. 2). Moreover, contrary to the conventional wisdom, increase of peer degree from 1 to 2 and 3 further reduces the fraction of superpeers in the network which makes networks with $k_l = 2, 3$ more vulnerable.
2. However as peer degree increases beyond 4, the peers sometimes connect among themselves and are not entirely dependent on superpeers for connectivity. Hence stability of the network increases (Fig. 2).

5. CONCLUSION

The main contribution of the paper lies in development of the common analytical framework to evaluate the robustness of p2p networks against various disturbances. Besides giving a quantitative measure of stability, the analytical framework also provides some interesting results. It formally explains the reason behind the stability of the superpeer networks against churn and points out its fragility to targeted attack. Several fine tuned disruption models like degree dependent failure and attack can be investigated further.

6. REFERENCES

[1] S. Saroiu, P. K. Gummadi, S. D. Gribble : "Measuring and Analyzing the Characteristics of Napster and Gnutella Hosts", Multimedia Systems Journal, 8(5), Nov. 2002.

[2] M. E. J. Newman, S. H. Strogatz, D. J. Watts : "Random Graphs with Arbitrary Degree Distributions and Their Application", Physical Review E, 2001.