How stable are large superpeer networks against attack?

Bivas Mitra Sujoy Ghose Niloy Ganguly
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur, India
{bivasm, sujoy, niloy}@cse.iitkgp.ernet.in

Abstract

In this paper, we analyze the stability of large scale superpeer networks against attacks. Two different kinds of attacks namely deterministic and degree dependent attack have been introduced. We model the superpeer networks with the help of bimodal degree distribution and different attacks with the help of graph dynamics. It is interesting to observe from both theoretical and simulation results that peer degree plays the key role for maintaining the stability of the network in face of these two attacks.

1 Introduction

Understanding the effect of attacks upon the large scale superpeer networks is becoming a major challenge in front of p2p network community. The most prominent attack that affects the stability of the network is Denial of Service (DoS) attack [1]. In the p2p networks, DoS drown important peers in fastidious computation so that they fail to provide any service requested by other peers. In this paper, we measure the stability of superpeer networks against various kinds of attacks. *Attacks are modeled in terms of removal of important nodes from the network.* We characterize the importance of a node mainly by its connectivity and bandwidth. The peers and superpeers in the network connect among themselves to form a single *giant component*. Disintegration of this giant component helps us to measure the stability of the attacked network. We also perform simulation to validate the theoretical results.

2 Analytical framework

We use generating function to derive the general formula for measuring the stability of overlay structures undergoing any kind of disturbances in the network. 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 attack. We establish the relationship between stability and p_k and q_k using the generating function formalism [2]. The critical condition for the disruption of the giant component for any type of graphs (characterized by p_k) undergoing any type of disrupting event (characterized by $f_k = 1 - q_k$) becomes

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

3 Topology and attack models

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 $p_k > 0$ if $k = k_l, k_m$, otherwise $p_k = 0$.

Attack models are specified through the model parameter q_k.

1. Deterministic attack : Superpeer nodes are targeted before attacking any peer. Formally
$q_k = 0$ when $k > k_{max}$
$0 \leq q_k < 1$ when $k = k_{max}$
$q_k = 1$ when $k < k_{max}$
This removes a fraction of nodes from the network with degree $\geq k_{max}$.

2. Degree dependent attack : Both peers and superpeers are attacked simultaneously, but the probability of superpeers being attacked is much more than that of the peers. Formally the probability of removal of a node having degree k (f_k) is proportional to k^γ where $\gamma \geq 0$ is a real number.

Stability metric: The stability of superpeer networks are primarily measured in terms of certain fraction of nodes (f_c) called percolation threshold [3], removal of which disintegrates the network into large number of small, disconnected components.

4 Stability of superpeer networks against attack

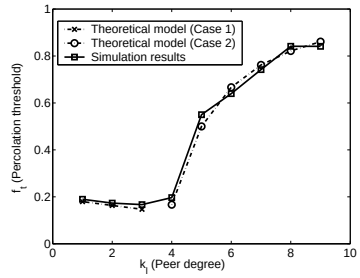
Stability analysis against deterministic attack

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

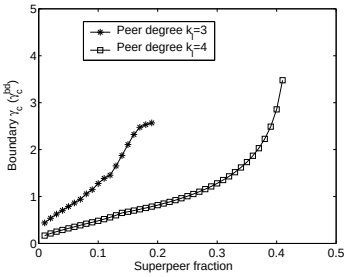
Case 1 : Removal of a fraction of superpeers is sufficient to disintegrate the network. The percolation threshold f_t for case 1 can be obtained from Eq. (1)

$$f_t = (1 - r)\left(1 - \frac{\langle k \rangle - k_l(k_l - 1)r}{k_m(k_m - 1)(1 - r)}\right) \qquad (2)$$

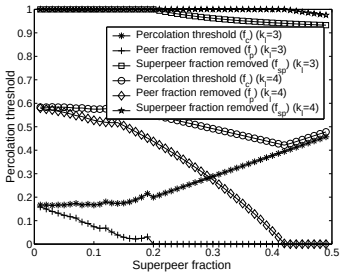
Case 2: Removal of all the superpeers is not sufficient to disintegrate the network. Therefore we need to remove



(a) Deterministic attack : The behavior of the superpeer network 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.



(b) Degree dependent attack : Superpeer networks with peer degrees $k_l = 3, 4$ average degree $\langle k \rangle = 5$ are considered. Behavior of γ_c^{bd} with respect to the change in superpeer fraction is shown.



(c) Degree dependent attack : Fraction of peers and superpeers required to be removed to breakdown the network and its impact upon percolation threshold f_c.

Figure 1. The above plots illustrate the impact of deterministic as well as degree dependent attack on superpeer networks.

some of the peer nodes along with the superpeers. The percolation threshold for case 2 becomes

$$f_t = r\left(1 - \frac{\langle k \rangle}{k_l(k_l - 1)r}\right) + (1 - r) \tag{3}$$

Observations: 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. 1(a)). 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. 1(a)).

Stability analysis against degree dependent attack
In this kind of attack, the critical condition for the stability of the giant component can be rewritten from Eq. (1) as

$$\begin{aligned} rk_l^{\gamma+1}(k_l - 1) + (1 - r)k_m^{\gamma+1}(k_m - 1) \quad &\geq \\ k_m^{\gamma}(\langle k \rangle(k_m + k_l) - k_m - 2\langle k \rangle) \end{aligned} \tag{4}$$

The solution set of the inequality (4) (say S_{γ_c}), which yields a set of values for γ, (γ_c, termed as critical exponent) can be bounded (where $0 \leq \gamma_c \leq \gamma_c^{bd}$) or unbounded (where $0 \leq \gamma_c \leq +\infty$). Each critical exponent γ_c specifies the fraction of peers and superpeers required to be removed ($f_p^{\gamma_c}$, $f_{sp}^{\gamma_c}$ respectively) to breakdown the network. Hence percolation threshold $f_c^{\gamma_c} = rf_p^{\gamma_c} + (1 - r)f_{sp}^{\gamma_c}$. The nature of the solution set S_{γ_c} has profound impact upon the behavior of $f_p^{\gamma_c}$, $f_{sp}^{\gamma_c}$ and as well as $f_c^{\gamma_c}$. The breakdown of the network can be due to one of the three situations noted below

Case A : Removal of all the superpeers alongwith a fraction of peers. Networks having bounded solution set S_{γ_c} where $0 \leq \gamma_c \leq \gamma_c^{bd}$ exhibit this kind of behavior at the maximum value of the solution $\gamma_c = \gamma_c^{bd}$.
Case B : Removal of only a fraction of superpeers. Some networks have open solution set S_{γ_c} where $0 \leq \gamma_c \leq +\infty$. At $\gamma_c \to \infty$, $f_p^{\gamma_c}$ converges to 0 and $f_{sp}^{\gamma_c}$ converges to some x where $0 < x < 1$.
Case C : Removal of some fraction of both superpeers and peers. Intermediate critical exponents $\gamma_c \in S_{\gamma_c}$ signifies the fractional removal of both peers and superpeers.
Observations: Solution set of the networks upto a threshold superpeer fraction sp^{th}, ($sp^{th} = 0.19$ and 0.41 for $k_l = 3$ and $k_l = 4$ respectively) remains bounded (Fig. 1(b)). Hence the removal of all the superpeers is necessary to disintegrate the network along with a fraction of peers (Fig. 1(c)). It also represents some instances of case B where only some fraction of superpeers are needed to be removed.

5 Conclusion

It can be observed that case A and case B of the degree dependent attack resembles with case 1 and case 2 of deterministic attack. Hence degree dependent attack model provides us with a more general scenario where various situations can be obtained only by changing the parameter γ.

References

[1] Baptiste Pretre : "Attacks on Peer-to-Peer Networks", Ph.D thesis, Swiss Federal Institute of Technology (ETH) Zurich, 2005.

[2] Bivas Mitra, Fernando Peruani, Sujoy Ghose and Niloy Ganguly, Measuring Robustness of Superpeer Topologies, PODC 2007, Portland, USA, (Brief Communication)

[3] 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.