Ubiquitous Computing

Attack and stability of superpeer networks

Generalized Theory for node disruption, analyzing the vulnarability.

Amartya Khan

Sangam Jain

Rishav Mishra

1. Introduction

In this chapter, we propose another analytical framework to understand the impact of different types of attacks on superpeer networks. There are many results that have been derived for infinite networks, however, little is known about the stability of finite size networks. The framework developed in this chapter sheds some light on finite size network by proposing an alternative expression for the percolation threshold.

2. Development of Analytical Framework

In this section, we present the detail derivation of the critical condition for measuring the stability of peer to peer networks undergoing any kinds of attacks. We start out by repeating some definitions mentioned before. Let p_k be the probability of finding a node chosen uniformly at random with degree k. Let f_k be the probability that a node of degree k is removed after the attack. Correspondingly $1 - f_k$ is the probability that a node of degree k survives the attack. In our framework, degree distribution p_k models the ensemble of p2p topologies and f_k models the disruptive events that take place in the network.

2.1. Deformed topology after attack

Now, we theoretically compute the degree distribution of the deformed topology p'_k after performing an attack on the p2p network of size N with initial degree distribution p_k. The first step in the attack is to select the nodes that are going to be removed according to the probability distribution f_k. Thus we have two subsets of surviving nodes S and removed nodes R.

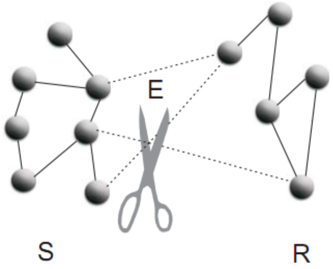

Figure 4.1: The scheme illustrates an attack as consisting of two steps: selection of nodes to be removed (set of removed nodes, R), and cutting of the edges E that run from the surviving nodes (set of surviving nodes, S) to the set of removed nodes R. As the scheme shows, the attack affects the degree of the surviving nodes.

The degree distribution of the surviving subset S is $(1 - f_k)p_k$ while the subset of nodes to be removed R (that is the edges connecting set S and set R) still exist. However, when these nodes are actually removed, the degree distribution of the surviving nodes S is changed due to the removal of the E edges that run between these two subsets.

total number of edge tips/ half edges in the surviving subset S including E links that are goingto be removed can be expressed by the sum $\sum_{j=0}^{\infty} j\, n_j\, (1 - f_j)$ where $n_j = Np_j$ is the total number of nodes in the network having degree j.

kn_kf_k= total number of edge tips connected with all the k degree nodes in R.

$\sum_k kn_kf_k$ = total number of tips in R.

The probability of a randomly chosen tip to be removed is = $\frac{\sum_k kn_kf_k}{\sum_k kn_k}$.

the probability of a randomly chosen tip of an edge to be removed (i.e. member of set R) and another tip of that edge being connected to either set S or R becomes:

$\frac{\sum_k kn_kf_k}{\sum_k kn_k - 1}$ (since a tip cannot be connected to itself).

As the network is uncorrelated, it is equally probable that the other end of the removed tip (member of set R)is connected to the nodes of set S or set R. Assuming this unbiasness, the total number of edge tips in set R connected to the nodes of the set S can be expressed as:

$$E = \left(\frac{\sum_{i=0}^{\infty} i\, n_i\, f_i}{\left(\sum_{k=0}^{\infty} k\, n_k\right) - 1} \right) \sum_{j=0}^{\infty} j\, n_j\, (1 - f_j)$$

The probability ϕ of finding an edge in the surviving subset S ,that is connected to a node of the other subset R :

$$\phi = \frac{E}{\sum_{i=0}^{\infty} i\, n_i\, (1 - f_i)} = \frac{E}{N \sum_{i=0}^{\infty} i\, p_i\, (1 - f_i)} = \frac{\sum_{i=0}^{\infty} i\; p_i\; f_i}{\left(\sum_{k=0}^{\infty} k\, p_k\right) - 1/N}$$

The probability p^s_q of finding a node with degree q in the surviving subset S (before cutting the E edges) simply becomes:

$$p_q^s = \frac{(1 - f_q)p_q}{1 - \sum_{i=0}^{\infty} p_i f_i}$$

The removal of nodes can only lead to a decrease in the degree of a survived node. If we find a node of degree k that has survived, it can be due to the fact that originally its degree was k + q and k of its edges survived while q (q may be zero also) got removed. Hence:

$$p'_k = \sum_{q=k}^{\infty} \left(\begin{array}{c} q \\ k \end{array} \right) \phi^{q-k} (1-\phi)^k \, p^s_q$$
.

2.2. Critical condition for stability

Now we derive the critical condition for stability of the peer to peer networksafter attack. In order to do that, we utilize the expression of the deformed degree distribution p'$_k$ after removal of nodes.

$$\kappa' = \frac{\langle k^2 \rangle'}{\langle k \rangle'} > 2$$

where <k>'and <k^2>' are the first and second moments of the degree distribution after the attack. The critical condition k' = 2 determines the point at which the network breaks down

After some calculation, the critical condition of stability in any large scale uncorrelated peer to peer networks is:

$$\sum_{k=0}^{\infty} k p_k (k(1-f_k) - (1-f_k) - 1) = 0$$
.

3. Effect of attack on stability

Now we formally analyze the effect of attacks on the superpeer networks with the help of the developed framework. Two kinds of attacks are possible, namely deterministic attack and degree dependent attack.

3.1. Deterministic Attack

We consider superpeer networks with peer degree k$_l$ = 2 and superpeer degree k$_m$ =20 and assume that 80% of nodes in the network are peers. Suppose 10% of nodes are removed through deterministic attack which signifies that 50% of superpeers get removed. We calculate the new degree distribution after attack (p'$_k$) .

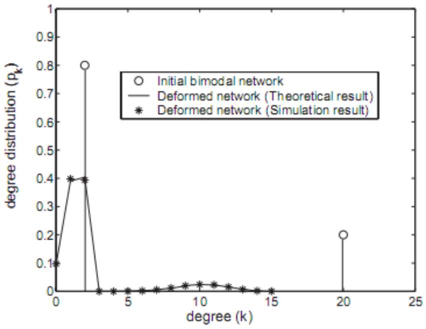

Figure 4.2: Topological deformation of the superpeer networks in face of deterministic attack. After the attack, 10% of nodes are removed. This 10% of nodes correspond to the 50% of the superpeer nodes whose degree is 20. The initial bimodal network and deformed network after attack are shown in the figure. The theoretically calculated degree distribution (p'_k) is verified through simulation.

Stability of the superpeer networks is challenged by attack on prominent peers or superpeers. In this section, we analyze the effect of this kind of targeted attack upon superpeer networks where r is the fraction of peers and rest are superpeers. In the case of targeted attack two cases may arise:

Case 1 Removal of a fraction of superpeers is sufficient to disintegrate the network.

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.

We analyze these two cases with bimodal network:

the critical condition for the stability of the superpeer networks can be rewritten as:

$$\sum_{k=k_l,k_m} k(k-1)p_k q_k = \langle k \rangle$$

The equation can be further expanded as below to differentiate between peers and superpeers:

$$k_l(k_l-1)p_{k_l}q_{k_l} + k_m(k_m-1)p_{k_m}q_{k_m} = \langle k \rangle$$

Case 1: In this case, removal of a fraction of superpeers is sufficient to disintegrate the network. If f_{sp} be the critical fraction of superpeer nodes, removal of which disintegrates the giant component, then $q_k = 1$ for $k = k_l$ and $q_k = 1 - f_{sp}$ for $k = k_m$.

$$\sum_{k=k_l} k(k-1)p_k + \sum_{k=k_m} k(k-1)p_k(1-f_{sp}) = \langle k \rangle$$

$$\Rightarrow f_{sp} = 1 - \frac{\langle k \rangle - k_l(k_l-1)p_{k_l}}{k_m(k_m-1)p_{k_m}}$$

As the fraction of superpeer nodes in the network is (1−r), then percolation threshold for case 1 becomes:

$$f_{tar} = (1-r) \times f_{sp}$$

$$\Rightarrow f_{tar} = (1-r)\left(1 - \frac{\langle k \rangle - k_l(k_l-1)r}{k_m(k_m-1)(1-r)}\right)$$

Case 2: Here we have to remove fp fraction of peer nodes along with all the superpeers to breakdown the network. Therefore q_k =1 − f_p for k = k_l and q_k = 0 for k = k_m.

$$k_l(k_l-1)p_{k_l}(1-f_p) = \langle k \rangle$$

$$\Rightarrow f_p = 1 - \frac{\langle k \rangle}{k_l(k_l-1)p_{k_l}}$$

Therefore the total fraction of nodes required to be removed to disintegrate the network for case 2 becomes:

$$f_{tar} = rf_p + (1-r).$$

$$f_{tar} = r\left(1 - \frac{\langle k \rangle}{k_l(k_l-1)r}\right) + (1-r)$$

Transition point: The transition from case 1 to case 2 can be easily marked by observing the value of percolation threshold f_{tar}. if the value of ftar exceeds the fraction of superpeers in the network (1−r), it indicates that removal of all the superpeers is not sufficient to disrupt the network. Hence subsequently we enter into case 2 to find percolation threshold.

3.2. Impact of peer contribution

We consider the networks with k_l =1, 3, 5.

peer contribution Pr_C ($0.1 \leq Pr_C \leq 0.9$).

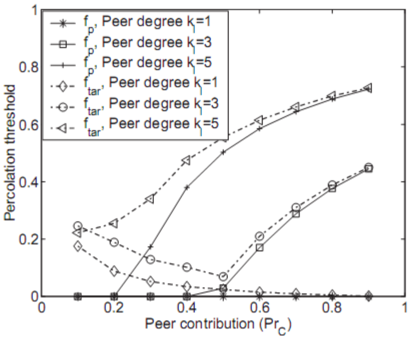

Figure 4.4: The plot represents the impact of peer contribution Pr_C upon the stability of the network against attack. f_p represents the fraction of peers required to be attacked to dissolve the network and f_{tar} indicates the corresponding percolation threshold.

Observations:

- It can be observed that superpeer networks having peer degree k_l = 1 can be disintegrated without attacking peers at all for any peer contribution Pr_C. This kind of attack belongs to case 1 of the attack model.

- The peers of the superpeer networks having peer contribution $Pr_C \leq 0.2$does not have any impact upon the stability of the network. This is true for low as well as high degree peers.

- The influence of high degree peers increases with the increase of peer contribution. At Pr_C =0.3, a fraction of peers is required to be removed to disintegrate the networks having peer degree k_l = 5. The impact of high degree peers upon the stability of the network becomes more eminent as peer contribution $Pr_C \geq 0.5$. In this region, a significant fraction of peers is required to be removed for all the networks having peer degree k_l =3, 5. This kind of attack belongs to case 2 of the attack model.

- For $Pr_C \geq 0.4$ brings the percolation threshold the stability of the networks is primarily dependent upon the stability of the peers.

- Pr_C has two opposite effects upon stability of the networks depending on the peer degree k_l. The percolation threshold ftar increases with peer contribution Pr_C for k_l =3, 5, but gradually reduces for 1. The reason behind this is, stability of the networks with peer degree k_l = 1 is entirely dependent upon superpeers. Since increase in peer contribution decreases superpeer contribution, it decreases stability of these networks also.

3.3. Degree dependent attack

In this kind of attack, the probability of removal of a node of degree k is directly proportional to k^{γ} where $\gamma \geq 0$ is a real number and represents the information available to the attacker about the topological structure of the network.

The probability of removal of a node is proportional to its degree:

$$f_k = \frac{k}{k_m+1} \text{ (so } \gamma = 1)$$

With proper normalization, probability of removal of a node having degree k becomes:

$f_k = \frac{k^{\gamma}}{C}$ where C is the normalization constant.

let r be the fraction of peers with degree k_l while rest are superpeers of degree km.If <k> is the average degree of the network,then:

$$p_{k_l} = r = \frac{k_m - \langle k \rangle}{k_m - k_l} \qquad p_{k_m} = (1-r) = \frac{\langle k \rangle - k_l}{k_m - k_l}$$

Thus, the critical condition for the stability of the giant component can be rewritten as:

$$\sum_{k=k_l,k_m} k(k-1)p_k(1-f_k) = \langle k \rangle$$

$$\Rightarrow \langle k^{\gamma+2} \rangle - \langle k^{\gamma+1} \rangle = C(\langle k^2 \rangle - 2\langle k \rangle)$$

$$\Rightarrow rk_l^{\gamma+1}(k_l-1) + (1-r)k_m^{\gamma+1}(k_m-1) =$$
$$C(\langle k \rangle (k_m + k_l) - k_m - 2\langle k \rangle)$$

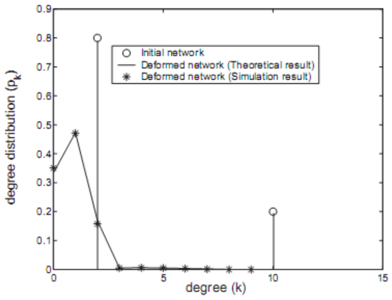

Figure 4.6: Topological deformation of the superpeer networks in face of degree dependent attack. The nodes are removed from the network with $f_k = \frac{k}{k_m+1}$. The initial bimodal network and the deformed network after attack p'_k are shown in the figure.

4. References

- Generalized theory for node disruption in finite-size complex networks, Physical Review E, 78, 026115, 2008.

- Analyzing the Vulnerability of the Super-peer Networks Against Attack, ACM CCS, 14th ACM Conference on Computer and Communications Security, Alexandria, USA, 29 October - 2 Nov, 2007