Attacks on Correlated Peer-to-Peer Networks: An Analytical Study

Animesh Srivastava
Department of CSE
IIT Kharagpur, India
asrivastava@cse.iitkgp.ernet.in

Bivas Mitra
CNRS
Paris, France
bivas.mitra@iscpif.fr

Fernando Peruani
MPI-PKS
Dresden, Germany
peruani@pks.mpg.de

Niloy Ganguly
Department of CSE
IIT Kharagpur, India
niloy@cse.iitkgp.ernet.in

***Abstract*—Analysis of attacks on real-world p2p networks and their impact on the topology of the network is difficult as the interconnections among the peers are not random; rather they evolve based on the needs of the connected peers and this brings in degree-degree correlation in the network. We develop an analytical framework to analyze the change in topology of a correlated network and propose a generalized model based on percolation theory to measure the resilience of a correlated network against any arbitrary attack. We present the results and analysis mainly on correlated superpeer networks and correlated bimodal networks. Some of the intricate questions on the stability of real-world superpeer network that we answer analytically are: (a) dependence of percolation threshold of a superpeer network on its peer degree, superpeer degree at different levels of degree-degree correlation (b) minimum peer degree required to make a superpeer topology more resilient. All our theoretical results are validated through simulations and the results are in very good agreement.**

I. Introduction

Popular peer-to-peer networks like Gnutella, Kazaa are increasingly subjected to various kinds of attacks like Denial of Service attack (DoS), DDoS attack, Eclipse attack, Sybil attack etc [1]. All these attacks try to interrupt the network-wide peer communication by disrupting the activities of the highly connected (resourceful) nodes. Besides, the continuous churn of the constituent nodes may also lead to interruption in the network-wide communication. Analytical work predicting the outcome of such churn and attack on large dynamic networks has been studied in depth [2]–[5], in the last decade. The results are primarily based upon the concept of percolation theory whereby the relation between component size and attack is established. These works have been successfully extended in the domain of p2p networks [6], [7], where Mitra *et al.* developed a generalized analytical framework to measure the deformed degree-distribution and stability of uncorrelated superpeer networks. (Note: Most of the popular p2p networks maintain a superpeer architecture comprising of some very powerful ultrapeers and the rest low bandwidth peers). However, we observe that although the framework quite accurately predicts the changes in Gnutella[1] (taken as representative real-life superpeer network) topology under random failure (fig. 1(a)), there is a distinct deviation in case of intentional attack (fig. 1(b)).

Current research reveals that superpeer networks (like most real networks) evolve through the complex and unsupervised interactions among peer nodes and this eventually leads to network heterogeneity. These complex interactions among the peers of the network make the vulnerability analysis very difficult as they behave differently under given conditions. For example, it has been observed in many real networks, that a relatively localized damage in one network may lead to failure in another, triggering a disruptive avalanche of cascading and escalating failures. In [9], Vespignani showed that this kind of dangerous vulnerability is indeed due to the heterogeneity present in the network. In [10], Buldyrev *et al.* addressed this issue and showed that analyzing complex systems as a set of interdependent networks destabilizes the most basic assumptions that network theory has relied on for single networks. Hence, in the design of resilient infrastructures, understanding the fragility induced by multiple interdependencies is presently one of the major challenges.

In superpeer networks, beyond the heterogeneity of degrees, it is observed that the interconnections between the nodes are not entirely random; rather "disassortative". For example high-degree nodes tend to be connected to low-degree nodes [11]. The real-world representative snapshots of commercial Gnutella networks accordingly exhibits negative degree correlation with assortativity coefficient $r = -0.792$. Hence to understand the exact impact of attacks, the interdependence of degree heterogeneity and degree-degree correlation need to be taken into consideration.

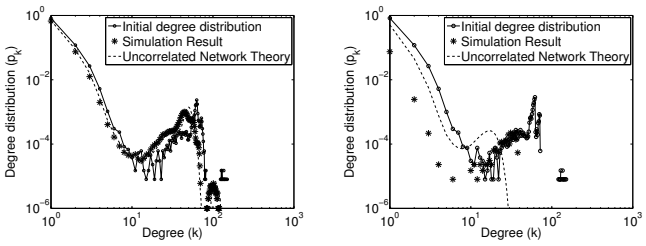
In order to achieve that, we propose a generalized framework for correlated network using tools from percolation theory and the apparatus of generating functions. We show that our framework is able to correctly assess the network properties like topological deformation as well as estimate the resilience of the network. We show that the framework can be applied to real-world networks by accurately predicting the topology deformation in the simulated real-world Gnutella network.

II. Environment Definition

Apart from using the snapshot of Gnutella network, we model the superpeer networks with bimodal network for our

[1]The snapshots have been obtained from the Multimedia & Internetworking Research Group of University of Oregon, USA [8]. The snapshot is obtained by the research group during September 2004 and the size of the network simulated from the snapshot is of $1,31,869$ nodes.

978-1-4244-9920-5/11/$26.00 ©2011 IEEE



(a) (b)

Fig. 1. Effect of attack and failure upon the Gnutella network simulated from the topological snapshot taken during September 2004. (a) The degree distribution of the deformed Gnutella network after random failure. Here 20% of the nodes are removed from the network randomly. (b) The degree distribution of the deformed Gnutella network after deterministic attack. Here all the nodes in the network having degree greater than 40 are removed.

simulation based experiments. In this section, we provide a brief description of the modeling of different network topologies and attacks. In addition, we also provide the formal representation of the network assortativity as a manifestation of network heterogeneity.

A. Modeling Superpeer Network Topologies

It has been observed that the superpeer networks follow bimodal degree distribution that sharply deviates from the power law behavior of scale free networks [6], [12]. Rigorous simulation results show that both of these networks namely bimodal networks and superpeer networks exhibit similar qualitative behavior under various node disturbances like churn and intentional attack. Therefore we believe bimodal network is simple enough to understand; at the same time it captures the essential features of superpeer networks. In bimodal network, a small fraction $(1-\alpha)$ of high degree (k_m) superpeers are connected with a large fraction (α) of low degree (k_l) peer nodes. Hence $p_{k_l} = \alpha$ and $p_{k_m} = (1-\alpha)$.

B. Attack Model

The attacks on a network are modeled in terms of different node removal strategies. Let f_k be the probability by which a node of degree k is removed from the network. In this paper, we primarily concentrate on **deterministic attack** where nodes having high degrees are progressively removed. Formally

$f_k = 1$ when $k > k_{cut}$
$0 \leq f_k < 1$ when $k = k_{cut}$
$f_k = 0$ when $k < k_{cut}$.

This removes all the nodes from the network with degree greater than k_{cut} and a fraction of nodes having degree equal to k_{cut}. Kindly note that, $f_k = f$ represents the degree independent attack or **random failure**. In random failure, the removal of any randomly chosen node having degree k after the attack is constant and independent of its degree k.

C. Assorativity

A correlated network can be completely defined by its degree distribution p_k and a degree-degree correlation matrix P (Matrix 1), where an element $P(i,j)$ defines the probability of finding an edge emerging from an i degree node to a j degree node.

$$P = \begin{pmatrix} P(1,1) & P(1,2) & ... & P(1,k_{max}) \\ P(2,1) & P(2,2) & ... & P(2,k_{max}) \\ . & . & . & . \\ . & . & . & . \\ P(k_{max},1) & P(k_{max},2) & ... & P(k_{max},k_{max}) \end{pmatrix}$$

Matrix 1: Degree-degree correlation matrix

In case of an undirected network the probability that a node of degree i and a node of degree j gets connected is same as that of a node of degree j getting connected with a node of degree i. Hence,

$$P(i,j) = P(j,i) \ for \ undirected \ graph \tag{1}$$

The probability of finding an edge with an i degree node at least at one end is given by the sum of the elements of the i^{th} row of the matrix P and it can be expressed as

$$\sum_j P(i,j) = \frac{i.p_i}{\sum_k k.p_k} = \frac{i.p_i}{\langle k \rangle} \tag{2}$$

Interestingly, the definition of degree-degree correlation matrix can be applied to random networks (that have no degree-degree correlation), where the probability of an edge emerging from i degree node to j degree node is the probability of selecting one tip of degree i and one tip of degree j. Formally, for random networks

$$P(i,j) = \frac{i.p_i}{\langle k \rangle} . \frac{j.p_j}{\langle k \rangle} \tag{3}$$

The assortativity coefficient r, the measure of degree-degree correlation, of a network lies in the range $-1 \leq r \leq 1$ and can be computed from the matrix P using the expression proposed by Newman [11] as

$$r = \frac{\sum_{j,k} jkP(j,k) - [\sum_{j,k} (\frac{j+k}{2}) P(j,k)]^2}{\sum_{j,k} (\frac{j^2+k^2}{2}) P(j,k) - [\sum_{j,k} (\frac{j+k}{2}) P(j,k)]^2} \tag{4}$$

III. Developing Analytical Framework for Correlated Networks

In this section, we present a formalism to analyze the topological deformation and resilience of the correlated network undergoing any kinds of attacks. We are going to establish the relationship between stability, p_k and f_k using the degree-degree correlation matrix P. This is done as a two step process; in the first step, we calculate the degree distribution of the deformed network. In the second step, we derive the critical condition of stability of p2p networks against attack.

A. Deformed Topology after attack

Here, we theoretically compute the degree distribution of the deformed topology p'_k after performing an attack on the correlated p2p network of size N with initial degree distribution p_k. We first select the nodes that are going to

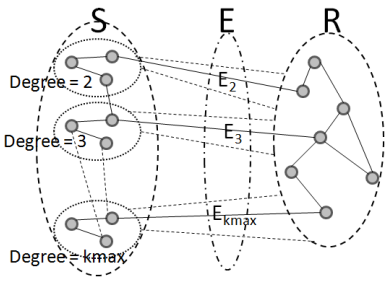


Fig. 2. Dissection of a correlated network into two sets S and R due to the attack on the network.

be removed according to the probability distribution f_k and then divide the network into two subsets, one subset contains the surviving nodes (S) while the other subset comprises of the nodes that are going to be removed (R). This is illustrated in fig. 2. 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 exists. However, when these nodes are actually removed, the degree distribution of the surviving nodes in S is changed due to the removal of the E_j edges, for every degree j, that run between nodes of degree j in the surviving set S and any node of the removed set R.

To calculate the degree distribution after the attack, we have to estimate $E = \sum_{j=0}^{k_{max}} E_j$, which is the total number of edges running between set S and R. The expression for E_j can be formulated in the following way. A node of degree k has k tips to which an edge can be attached and the total number of tips present in the network, $S \bigcup R$, is $N \cdot \langle k \rangle$. A fraction of these tips are j degree tips that are connected to k degree tips and can be expressed as $N \cdot \langle k \rangle \cdot P(j,k)$. We know, the probability that a node of degree j lies in set S and a k degree node lies in set R are $(1-f_j)$ and f_k respectively. Therefore, the number of edges connecting a node of degree j in the set S and a node of degree k in the set R becomes $N \cdot \langle k \rangle \cdot P(j,k) \cdot f_k \cdot (1-f_j)$. This helps us in deriving the total number of edges whose one end is connected to j degree node in set S and the other end is connected to any node in set R, which is

$$E_j = N \cdot \langle k \rangle \cdot (1-f_j) \sum_k P(j,k) \cdot f_k \tag{5}$$

Using E_j we can calculate the probability ϕ_j of finding an edge running between a j degree node in the surviving set S and any node in the set R expressed as

$$\phi_j = \frac{E_j}{j \cdot N \cdot p_j \cdot (1-f_j)} \tag{6}$$

The term ϕ_j also signifies the probability that a j degree node loses one link due to the removal of E edges. Here we define the probability p_k^s of finding a node with degree k in the surviving set S (before removing the E edges) as

$$p_k^s = \frac{(1-f_k).p_k}{1 - \sum_i p_i.f_i} \tag{7}$$

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. The fraction of nodes having degree k after attack i.e. p'_k is given by the fraction of p_k^s nodes, who did not lose any link, and a fraction of p_{k+1}^s nodes who lost one link but rest k links survived, a fraction of p_{k+2}^s nodes who lost two links but rest k links survived and so on. Hence using the concept of binomial distribution and from the equations (6) and (7), we obtain the following expression for p'_k:

$$p'_k = \sum_{q=k}^{k_{max}} \binom{q}{k} \phi_q^{q-k} (1-\phi_q)^k \, p_q^s \tag{8}$$

(1) Special Case - Random failure: In this section we try to investigate the impact of a random failure attack on a correlated network and its deformed degree distribution. In case of random failure attack the probability of attack on every node is same i.e. $f_j = f_k = f\,(constant)$. Using $f_j = f_k = f$ and eq. (2) in eq. (5), the expression for E_j reduces to

$$E_j = f \cdot (1-f) \cdot N \cdot j \cdot p_j \tag{9}$$

We substitute the expression for E_j obtained from eq. (9) in eq. (6) and simplify ϕ_j as

$$\phi_j = \frac{f \cdot (1-f) \cdot N \cdot j \cdot p_j}{j \cdot N \cdot p_j \cdot (1-f)} = f \tag{10}$$

The deformed degree-distribution of the network due to random failure is obtained by using eq. (10) in eq. (8), expressed as

$$p'_k = \sum_{q=k}^{k_{max}} \binom{q}{k} f^{q-k} (1-f)^k \, p_q^s \tag{11}$$

Interestingly, the expression obtained in eq. (11) is exactly the same equation proposed in [7] for the deformed degree distribution of an uncorrelated network due to random failure. The above expression shows that degree-degree correlation has no role to play in case of random failure. This conclusion confirms the result shown in fig. 1(a) where we observe a good agreement of deformed topology obtained from the uncorrelated network theory [7] and simulation for Gnutella network.

(2) Special Case - Uncorrelated Networks: For uncorrelated networks, we use eq. (3) and eq. (5), to compute ϕ_j, the probability that a j degree node loses one tip, and the eq. (6) reduces to

$$\phi_j = \frac{\sum_k k \cdot p_k \cdot f_k}{\langle k \rangle} = \phi \tag{12}$$

The above expression shows that for uncorrelated networks, ϕ_j is independent of degree j and hence we denote it by ϕ. Using the reduced value of ϕ_j into the eq. (8) we get back the expression for deformed degree distribution of an uncorrelated network against any attack proposed in [7]. Hence our theory to predict the deformed degree-distribution of correlated networks against any attack can also be applied to the uncorrelated networks.

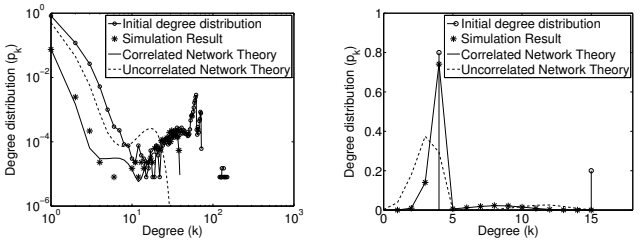


Fig. 3. (a) Effect on Gnutella network topology due to deterministic attack (by removing nodes with degree higher than 39). (b) Topological deformation of correlated bimodal network with assortativity coefficient of 0.81 due to the removal of 10% nodes deterministically. For both the cases simulation result is obtained as the average of 500 realizations.

B. Critical Condition for Stability

Our aim is to establish a relation between the percolation threshold (the measure of resilience), degree distribution p_k, correlation matrix P and the attack vector f_k for a correlated network. In order to achieve that, we follow the model developed by Goltsev *et al.* in [13] and customize it for developing a generalized stability criterion for a correlated network against any attack. We find that the stability (existence of giant component) of the deformed network depends upon the largest eigenvalue of a matrix called branching matrix B where

$$B(k,j) = (1-f_j)(j-1)P(k,j)\frac{\langle k\rangle}{k\,p_k} \tag{13}$$

After applying an attack f_k *if the largest eigenvalue of the matrix B is greater than or equal to* 1*, then there exists giant connected component*. This is the critical condition for the stability of a correlated network against any given attack.

IV. Experimental validation

In this section, we validate the theory derived for topology deformation and critical condition for stability of correlated network against various attacks through stochastic simulation. Based on the generation of the superpeer networks, the validation is done from two different perspectives, (a) simulating the real world Gnutella network (b) generating the superpeer networks from complex graphs.

A. Gnutella Network

To analyze the topology deformation due to deterministic attack we remove all the nodes with degree higher than 39. In fig. 3(a) we can see that our theory correctly predicts the topology deformation in the simulated real-world Gnutella network whereas the uncorrelated network theory fails to do so. Since the real-world network Gnutella is disassortative, the removal of one superpeer node leads to the removal of large number of peers. Hence, we expect that the Gnutella network can be disrupted very easily by applying deterministic attack, where the targeted nodes are of very high degree. The results are quite expected as the percolation threshold of the Gnutella network against deterministic attack obtained from theory and from simulation are 0.0204 and 0.0214 respectively, which means that removal of just 2% of nodes is enough to disintegrate the network.

B. Correlated Bimodal Networks

We have considered a bimodal superpeer network with peer degree 4, superpeer degree 15, assortativity coefficient 0.81 (highly assortative) and assumed that 80% nodes are peers. We remove 10% nodes which amounts to the removal of 50% superpeer nodes. The theory quite precisely predicts the deformed degree distribution as shown in fig. 3(b), and the percolation threshold of the network obtained from theory and from simulation are 0.71 and 0.73 respectively. When the stability of this network is measured at -0.49 assortativity, the theoretical as well as the simulation percolation threshold are found to be as low as 0.2.

Understanding Trends of Degree Deformation: In order to understand the impact of deterministic attack, we plot the deformed degree distribution of the bimodal network for various assortativity coefficient in fig. 4(a). We observe that as the network becomes more and more disassortative, the fraction of peers of degree 4 in the deformed network, represented by the peak at degree 4, decreases. Intuitively, we can explain the phenomena using the fact that in a disassortative network the interconnection among peers and superpeers is higher than that of in an assortative network. Hence, removal of a fraction of superpeer leads to removal of a higher number of edges from the peers. So, the peer degree begins to lose its modality and the distribution becomes flat at the region around the peer degree.

After the attack, a fraction of superpeers (degree h) that survived the attack lose exactly $(h-l)$ tips and become peers (degree l) causing increase in the number of peers. Using p^s_h, the probability of finding a degree h node in set S, from eq. (7) and ϕ_h, the probability that a h degree node loses a tip, from eq. (6), the increase in fraction of peers, l_{inc}, is expressed as

$$l_{inc} = \begin{pmatrix} h \\ h-l \end{pmatrix} \phi_h^{h-l}(1-\phi_h)^l\, p^s_h \tag{14}$$

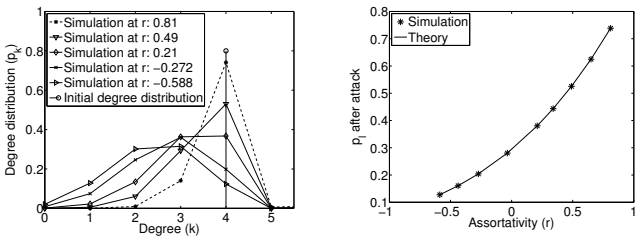
On the other hand $p_l \cdot f_l$ fraction of peers are removed due to the attack. From the rest of the peers, $p_l \cdot (1-f_l)$, a fraction of peers lose some tips resulting in decrease in the number of peers. The probability that a l degree node loses at least one tip is given by $(1-(1-\phi_l)^l)$. Therefore, the decrease in fraction of peers, l_{dec}, can be expressed as

$$l_{dec} = p_l \cdot f_l + p_l \cdot (1-f_l) \cdot (1-(1-\phi_l)^l) \tag{15}$$

Hence the probability of finding a peer after attack can be expressed as

$$p'_l = \frac{p_l - l_{dec} + l_{inc}}{\sum_k kp_k(1-f_k)} \tag{16}$$

As the network turns more and more disassortative, the probability ϕ_l that a peer will lose a tip increases, whereas the probability ϕ_h that a superpeer will lose a tip decreases. This in turn increases l_{dec} and decreases l_{inc} leading to overall decrease in p'_l. Using the theory, the change in fraction of peers



(a) (b)

Fig. 4. Effect of deterministic attack on the topology of a correlated bimodal network with 20% superpeers of degree 15 and 80% peers of degree 4. (a) Change in the deformed topology at different degree-degree correlations. (b) Change in fraction of peers after attack at different degree-degree correlation.

for same attack intensity at different degree-degree correlation has been predicted perfectly as shown in the fig. 4(b). We find that this change follows a parabolic path.

V. Case study: Attacks on Bimodal network

Equipped with the framework, that can accurately measure the impact of degree heterogeneity and degree-degree correlation on the superpeer networks, we determine the parameters that need to be understood to build resilient superpeer infrastructures. These parameters are:

(a) Properties of transition point: We define transition point as the configuration of a superpeer network where just the removal of superpeers is not sufficient to disrupt the network. Also as a corollary, the exact amount of peers to be removed beyond such points need to be determined.

(b) Critical assortativity: It is the assortativity at which a superpeer reaches the transition point.

(c) Critical peer degree: It is the peer degree below which the superpeer topology is fragile.

Bimodal networks, as stated in sec. II-A, are simplest yet reasonably accurate way to model superpeer networks and hence, helps us to analyze the aforementioned dominant resilience parameters at different degree-degree correlation under different intensity of deterministic attacks. Even though the results presented are on bimodal network topologies, they provide important insights while designing resilient generalized superpeer topologies.

For a given bimodal distribution with superpeer degree h, peer degree l and assortativity coefficient r, the degree-degree correlation matrix can be constructed from eq. (4). It is a symmetric matrix where the four non-zero entries are as follows:

$$P(l,l) = \frac{l.p_l(l.p_l + r.h.p_h)}{\langle k\rangle^2}$$
$$P(l,h) = P(h,l) = \frac{(1-r)l.p_l.h.p_h}{\langle k\rangle^2}$$
$$P(h,h) = \frac{h.p_h(r.l.p_l + h.p_h)}{\langle k\rangle^2}$$

Using this matrix we determine the corresponding branching matrix B. At the critical condition of stability, when the largest eigen value of matrix B is 1, the deterministic attack on the bimodal network leads to the following two cases that can be computed from eq. (13):

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

$$f_h = 1 - \frac{(l-1)(l.p_l + r.h.p_h) - \langle k\rangle}{(h-1)[r(l-1) - (r.l.p_l + h.p_h)]} \quad (17)$$

As the fraction of superpeer nodes in the network is p_h, the percolation threshold f_c for case 1 becomes $p_h \cdot f_h$.

2 Removal of all the superpeers is not sufficient to disintegrate the network. Therefore, we need to remove some of the peer nodes, f_l, along with the superpeers.

$$f_l = 1 - \frac{\langle k\rangle}{(l-1)(l.p_l + r.h.p_h)} \quad (18)$$

As the fraction of superpeer nodes in the network is p_h and fraction of peers is p_l, the percolation threshold for case 2 becomes $f_c = p_l \cdot f_l + p_h$.

(a) Transition Point: The transition point which is the transition from case 1 to case 2 can be easily marked by observing the value of the percolation threshold f_c. While calculating, if the value of f_c exceeds the fraction of superpeers in the network (p_h), it indicates that removal of all the superpeers is not sufficient to disrupt the network. The behavior of percolation threshold with respect to various assortativity coefficient is noted in fig. 5(a). The curves showing percolation threshold values beyond 0.2 indicate that peers have to be removed beyond superpeers to breakdown the network. It is observed that the network becomes more resilient as we increase the assortativity. It is also observed that beyond a certain peer degree (here 5) for the superpeer degree 15, it becomes impossible to break the network by removing just the superpeers, at any assortativity coefficient. Typically it is observed that the superpeer degree to peer degree ratio, $(h:l)$, needs to be above 3 for the attacker targeting only the superpeers to be successful.

(b) Critical Assortativity Coefficient r_c: The parameter r_c, is the assortativity at transition point and can be computed from eq. (17) as,

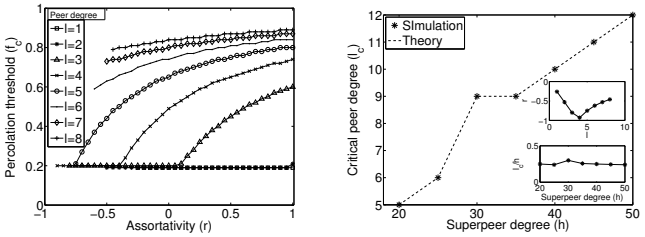
$$r_c = \frac{1}{l-1} - \frac{l.p_l(l-2)}{h.p_h(l-1)} \quad (19)$$

At peer degree $l = 1$, the value of r_c from eq. (19) becomes undefined, whereas at peer degree $l = 2$, the critical value is 1. This is the position where all the 2 degree nodes participate to form a giant component and remain unaffected by the removal of all the superpeers. In both the cases, r_c is independent of the superpeer degree h. When the parameters h, p_h and p_l are kept constant, the eq. (19) reduces to

$$r_c \approx \frac{1}{l} - K.l \quad (20)$$

where K is a constant. This shows that the r_c is inversely proportional to the peer degree l. This is in line with the observation in fig. 5(a).

(c) Minimum Assortativity Coefficient r_{min}: Even though the theoretical minimum value that the assortativity coefficient of a network can take is -1, for some bimodal configuration it is not possible to generate the network below a certain



(a) (b)

Fig. 5. Effect of deterministic attack on bimodal network with superpeer degree $h = 15$ and fraction of peers $p_l = 0.8$. The peer degree has been varied from 1 to 8.(a) Effect of deterministic attack at different assortativity coefficient. (b) Critical peer degree at different superpeer degree.

assortativity coefficient r_{min}. This can be easily marked by observing the emergence of negative entries in the generated degree-degree correlation matrix P for the bimodal network. A bimodal configuration with $r_c < r_{min}$ indicates that even the most disassortative network of the given configuration can not be disrupted by removing all the superpeers and hence the knowledge of r_{min} for a bimodal configuration is a very important parameter in determining the resilience against deterministic attack. We have computed r_{min} for all the bimodal configuration considered in our case and are shown in the inset of fig. 5(b). The assortativity coefficients at which different feasible bimodal configuration appear are shown in fig. 5(a). For example, the first feasible configuration for the network with superpeer degree 15 and peer degree 8 is at around -0.45 assortativity instead of -1. Also, note that for $l \geq 6$ even the first feasible configuration ensures a stable setting.

(d) Peer Degree l_c for a Superpeer Degree h: Since, for a bimodal network, r_c depends upon the peer degree l, we determine critical peer degree, l_c (for a given superpeer degree h), at which removal of all the superpeers are insufficient to disrupt the network and this happens when $r_c < r_{min}$. Hence the eq. (19) can be written as

$$r_{min} > \frac{1}{l_c - 1} - \frac{l_c . p_{l_c}(l_c - 2)}{h . p_h (l_c - 1)} \tag{21}$$

Using the eq. (21) we have theoretically computed the critical peer degree l_c for superpeer degree $20 \leq h \leq 50$ with 80% nodes as peers and compared it with the simulation result. The comparison in fig. 5(b) shows that the results are in excellent agreement. Interestingly, the ratio $\frac{l_c}{h}$ (shown in the inset of fig. 5(b)) shows some sort of invariance.

(e) Remaining Network Size Beyond Transition Point: Beyond transition point, in a superpeer network at $r = 1$, the fraction of peers to be removed in order to breakdown the entire network can be computed from the eq. (18) as

$$f_l = 1 - \frac{1}{l - 1} \tag{22}$$

In other words, at percolation threshold beyond transition point, with the increase in peer degree l for a given completely assortative bimodal configuration $(r = 1)$, the fraction of peers removed increases which in turn decreases the remaining number of peers in the network. It can be seen in the fig. (5(a)), at $r = 1$, the percolation threshold increases with the increase in peer degree l. Hence it can be said that beyond transition point the remaining network size is inversely proportional to the peer degree.

VI. Conclusion

This paper is a small but important step towards understanding the interplay of various complex interdependencies acting on large dynamic networks. It develops a generalized analytical framework in order to understand the impact of degree-degree correlation on the resilience of large scale superpeer network topologies and makes important observations. The interesting findings of the paper are: (a) For a superpeer network topology, there may exist a critical assortative mixing r_c beyond which it is impossible to disrupt the network even by removing all the superpeers, (b) Critical assortativity r_c is independent of superpeer degree for peer degree 1 and 2, whereas it becomes inversely proportional to peer degree $l \geq 3$, (c) For a superpeer network configuration, there exists a critical peer degree l_c above which the network remains resilient to targeted attacks, and (d) The critical peer degree to superpeer degree ratio is an important invariant which can be used to measure the resilience. Thus we have identified the parameter space which when considered in the design methodology of superpeer topologies can lead to resilient infrastructures.

References

[1] B. Pretre, "Attacks on peer-to-peer networks," Ph.D. dissertation, 2005.

[2] R. Cohen, K. Erez, D. Avraham, and S. Havlin, "Resilience of the internet to random breakdown," *Physical Review Letters*, vol. 85, no. 21, 2000.

[3] ——, "Resilience of the internet under intentional attack," *Physical Review Letters*, vol. 86, no. 16, 2001.

[4] M. E. J. Newman, S. H. Strogatz, and D. J. Watts, "Random graphs with arbitrary degree distributions and their application," *Physical Review E*, 2001.

[5] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts, "Network robustness and fragility: Percolation on random graphs," *Physical Review E*, vol. 85, no. 21, 2000.

[6] B. Mitra, F. Peruani, S. Ghose, and N. Ganguly, "Analyzing the vulnerability of superpeer networks against attack," in *CCS '07: Proceedings of the 14th ACM conference on Computer and communications security*. New York, NY, USA: ACM, 2007, pp. 225–234.

[7] B. Mitra, N. Ganguly, S. Ghose, and F. Peruani, "Generalized theory for node disruption in finite-size complex networks," *Phys. Rev. E*, vol. 78, no. 2, p. 026115, Aug 2008.

[8] Gnutella, "Gnutella snapshot." [Online]. Available: http://mirage.cs.uoregon.edu/P2P/info.cgi

[9] A. Vespignani, "Complex networks: The fragility of interdependency," *Nature*, vol. 464, pp. 984–985, Apr. 2010.

[10] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, pp. 1025–1028, Apr. 2010.

[11] M. E. J. Newman, "Assortative mixing in networks," *Phys Rev. Lett.*, vol. 20, no. 208701, 2002.

[12] B. Yang and H. Garcia-Molina, "Designing a super-peer network," *Data Engineering, International Conference on*, vol. 0, p. 49, 2003.

[13] A. V. Goltsev, S. N. Dorogovtsev, and J. F. F. Mendes, "Percolation on correlated networks," *Phys. Rev. E*, vol. 78, no. 5, p. 051105, Nov 2008.