Research of a Small World Architecture and Frangibility for P2P Networks

Yuhua Liu
Department of Computer Science, Huazhong Normal University, Prof., CCNU
Email: yhliu@mail.ccnu.edu.cn

Yongwei Meng, Kailhua Xu and Hongcai Chen
Department of Computer Science, Huazhong Normal University, Prof., CCNU
Email: ywmeng@yahoo.cn, xukh@phy.ccnu.edu.cn,hongcai@mails.ccnu.edu.cn

Abstract—P2P networks were new stars of 21 century and they were widely used in nowadays networks. It was factually an overlay network for distributed object store, search and sharing. But P2P networks frequently lacked of dependable, some peer nodes could be easily lost. So it was very important to study the architecture and frangibility of p2p networks and know the characteristics when nodes invalidated or suffered intentionally attacked which would be good used in future. In this paper, we presented a small world architecture for P2P networks for information discovery, peer nodes freely linked to each other in inter-groups and not every peer node needed to be connected to remote groups and also could easily find the information in remote peer node via some leader peer nodes. And analyzed the frangibility of Gnutella networks, including suffered random failure, degree attack and betweenness attack. And fully study the frangibility of p2p networks base on small world architecture (SWAN). From our analysis and simulation, the small world architecture for p2p networks had the same characters as small world networks, and could achieve good performance in both static and dynamic environments. And the SWAN was best fault tolerance when suffered randomly attack, but worst fault tolerance when suffered hostility attack compared with the ER model. And also the frangibility of p2p networks base on small world architecture was analyzed theoretically and a closed-form solution for average size of clusters was given which before the largest size of cluster had appeared.

Index Terms— P2P networks; small world architecture; Gnutella networks; frangibility; average size of clusters

I. INTRODUCTION

Peer-to-peer networks were distributed information sharing systems with no centralized control. Each node in a P2P networks had similar functionalities and played the roles of both a server and a client at the same time. The systems provided immense flexibility for users in performing application-level routing, data posting, and information sharing in the Internet. Oram gave a simple definition of peer-to-peer networks as: “P2P is a class of applications that take advantage of resources storage, cycles, content, human presence available at the edges of the Internet. Because accessing these decentralized resources means operate outside the DNS and have significant or total autonomy of central servers.”

Recently, researchers had been working on distributed structured P2P networks. Noted works included Chord, Tapestry, and Pastry. By applying the techniques of consistent distributed hashing and structured routing, these structured networks improved the efficiency of object lookup and reduced the amount of query traffic inside the network. The small world phenomenon, first proposed by Stanley Milgram, was the hypothesis that everyone in the world could be reached through a short chain of social acquaintances. T. Hong had observed this small world phenomenon in existing P2P networks. Duncan Watts proposed a mathematical model to analyze the small world phenomenon in highly clustered networks consisting of local nodes and random long-range shortcuts that helped produce short paths to remote nodes. Duncan demonstrated that the path length between any two nodes of his model graph was surprisingly small. Due to the similarity between the social networks and P2P networks, Duncan’s theory could be adopted in P2P networks that was each peer node was connected to same neighboring nodes, and a group of peer nodes together kept a small number of long links to randomly chosen distant peer nodes. The development of p2p networks technique and complex networks theory urged the deep study of topology of p2p networks. From the study of topology, we could know more about the weakness of the p2p networks, and design better one for protection and less danger.

This paper presented a small world architecture for P2P networks for information discovery, peer nodes freely linked to each other in inter-groups and not every peer node needed to be connected to remote groups and also could easily find the information in remote peer node via some leader peer nodes. It reduced the average distance and the lost of information and fault tolerant both in static and dynamic environments. This paper also studied the frangibility of Gnutella works, and the difference among ER model and p2p networks base on small world architecture, and also computed the average size of clusters before the largest size of cluster had

Manuscript received July 7, 2009; revised September 1, 2009; accepted September 28, 2009.
This research was supported by the natural science foundation of china(Grant No.60673163).
A. Small World Overlay In Peer-to-peer Networks

Most researches on constructing small world in peer-to-peer networks were based on the concept of clustering peer nodes into groups, communities, or cluster. Ken Y.k.Hui had built the small world overlay peer-to-peer protocol on top of existing structured P2P networks by classifying peer nodes into clusters, which achieved improved lookup performance over existing protocols. Liu used a rigorous binary tree code algorithm to improve search capability by organizing peer nodes into different peer groups, these group-based systems were built on top of structured peer-to-peer networks, acquired the efficiency of structured peer-to-peer protocols and achieved an enhanced performance. P. Triantafillou gave models which divided a Chord ring into smaller sub-rings to achieve better performances. However, these networks also inherited and even aggravated the problems of structured peer-to-peer networks by maintaining an additional multilayer topology.

B. Fault Tolerance In Peer-to-peer Networks

In peer-to-peer networks where nodes acted as both clients and servers, each peer provides the same set of functionalities, and the system behavior was obtained by the composition of the single behaviors. Therefore, the effectiveness of the whole system was strongly dependent upon the results provided by each single peer. In fact, a single peer leaving or failing was very popular, the common solution consists of providing multiple alternative routing paths for the same communication. Chord stored additional links to assure that at least low-performance routing was possible; CAN supported several mechanisms for replicating data and enabling searches across multiple directions; and Oceanstore relied on Tapestry which was a routing infrastructure storing additional links to guarantee fault-tolerance.

In this paper, we focused on robustness of connectivity and data availability based on the small-world network model, that, if one peer possessing many wide-range connections failed, the performance of the whole system could be very negatively affected.

C. Frangibility Of Gnutella Networks

Gnutella was a protocol for file share and distribution searches. Although this protocol also supported the traditional Client/Server searches criterion, but its main aim was peer to peer without center searches. According to the Gnutella criterion, when the Gnutella was finding messages, one node would send the requesting message to its neighbor node, the neighbor node would search the information whether suit for the requesting message, if it did, the neighbor node sent back a message, and checked the TTL of the requesting message, if the value of TTL was more than zero, then the neighbor node sent the requesting message to other nodes, if not, the neighbor node would stop sending message; else the neighbor node sent the requesting message to its neighbors.

Next we would show how to explore the topology of Gnutella by using order PING and PONG and the value of TTL. When node detector sent a PING order whose TTL value was 2 to its neighbor node, the neighbor node got the PING order and decreased its TTL value by 1, then sent the PING order to its neighbors, the lower neighbor nodes repeated the above operations until the TTL value reached zero, then the node sent back an order PONG to node detector. So the node detector got its neighbors’ IP information which in the second floor. Afterward, the node detector sent a PING order whose TTL value was 2 to the second floor neighbor nodes and repeated the operations. So the node detector got its neighbors’ information which in the third floor. And so on, we could get the whole topology by using such extent-preference ways.

We usually used network diameter and average shortest path to describe networks. The network diameter showed the power of communication for two nodes: the smaller diameter, the shorter length. A network with big number of nodes may possess small diameter, for example, a www network possessed 80,000,000 nodes, but its diameter was about 19. The average shortest path told the average time used to search the nodes.

Assumed that an intact Gnutella network was attacked, the topology was deeply destroyed that the whole network was divided into lots of unattached small clusters. So we analyzed the frangibility of Gnutella networks base on the maximal clusters, network centricity and network diameter. The maximal cluster was a relative size. The network centricity was defined by \( C_e = \frac{1}{\sum_{x \in U} d(x, y)} \), where \( d(x, y) \) denoted the shortest length between node x and y. U was the set of all nodes.

In order to know the results of frangibility of Gnutella networks, we used three ways to attack the networks that was random failure, degree attack and betweenness attack, and use f denote the percentage that nodes was removed. In experimentation, we got the following results.
III. A SMALL WORLD ARCHITECTURE FOR PEER-TO-PEER NETWORKS

A. Basic Definitions

In this section, we would provide basic definitions that clarified the concepts that would be used in the following sections. In the Duncan’s model, the small world networks were characterized by high clustering coefficients and short average path lengths. And the clustering coefficient of a node was defined as:

$$\gamma_v =\frac{|E(\Gamma_v)|}{C^2_{M_v}} \quad (1)$$

Where \(|E(\Gamma_v)|\) was the number of links in the neighborhood of \(v\), and \(C^2_{M_v}\) was the number of possible links in the neighborhood of \(v\). The clustering coefficient of small world architecture for p2p networks was analyzed in an n-node “graph” as show in Fig.1, where each peer node had k internal neighbors and \(i\) external neighbors \((n >> (k + i) >> 1)\), and peer groups which were connected by inter-group links do not overlap. Therefore, there were a total of \(k+1\) peer nodes in each group, and a total of \(g = \frac{n}{k+1}\) groups in the network. The publication and searching parameter \(d=0\) in the static environment of peer online rate \(p=100\%\). A peer node had \(i\) inter-group links. Therefore, it had \(k+i\) “neighbors” in the networks. The possible links between its neighbors were \(\frac{(k+i)(k+i-1)}{2}\). But in a static environment with \(d=0\), \(i\) external neighbors do not keep inter-group links to \(k\) internal neighbors. There were approximately \(\frac{i \cdot n}{2}\) inter-group links out of a total \(n(n-1)-n\cdot k\) possible links, where \(i\) was the average number of inter-group links. The probability that two external neighbors were connected to each other by an inter-group links was \(\frac{i}{n-k-1}\), which would close to 0. So the actual links in the neighborhood of a peer node were the links among its \(k\) internal neighbors: \(\frac{k(k+1)}{2}\).

And so the clustering coefficient of the peer node with \(i\) external neighbors was:

$$\gamma_i \approx \frac{2}{(k+i)(K+i-1)} \cdot \frac{(k(k-1))}{2}$$

$$=\frac{k(k-1)}{(k+i)(k+i-1)} \quad (2)$$

So the weighted average was:

$$\bar{\gamma} = \sum_{i=0}^{l} p_i \gamma_i$$

$$= \sum_{i=0}^{l} p_i \cdot \frac{k(k-1)}{(k+i)(k+i-1)} \quad (3)$$

where \(p_i\) was the probability that a peer node kept \(i\) external links, and \(l\) was the maximum of the inter-group links of a peer node.

The average path length \(L\) could be divided with two parts: \(d_{local}\) that was defined as the average distance between the peer nodes in inter-groups and \(d_{global}\) that was defined as the average distance for the peer nodes from different peer groups. Because each peer node needed one step to reach the other peer nodes in the same peer group except for itself, so \(d_{local} = \frac{k}{k+1}\), and \(d_{global}\) could be divided into three sub average distance \(d_{global} = H_1 + H_2 + H_3\), where 

\(H_1\): The average distance to get out of the starting group;

\(H_2\): The average distance to move between groups;

\(H_3\): The average distance to get into the requested group.

And we got

$$H_1 = 1 + \frac{k}{K+1} + \frac{1}{k+1} = \frac{k}{K+1}, \quad H_2 = 1,$$

$$H_3 = H_1, \quad so:\n$$

$$d_{global} = H_1 + H_2 + H_3 = \frac{k}{K+1} + 1 + \frac{k}{K+1}$$

$$= 1 + \frac{2k}{K+1} \quad (4)$$

The number of the pairs of peer nodes in a peer group was:

$$C^2_{k+1} = \frac{(k+1)(k+1)}{2} \quad (5)$$

And the total peer groups was \(g\), so the sum of pairs of peer nodes in the same peer group was:

$$N_{local} = \frac{(k+1)(k+1)}{2} \cdot g$$

$$= k(k+1) \cdot \frac{n}{k+1} = \frac{n(k+1)}{2} \quad (6)$$

The sum of the pairs between peer nodes inside and outside of peer groups in the whole network was:

$$N_{global} = C^2_n - N_{local} = \frac{n(n-k-1)}{2} \quad (7)$$

So the average path length between all pairs of peer nodes was:


\[ L = \frac{1}{N} (N_{local} \cdot d_{local} + N_{global} \cdot d_{global}) \]

\[ = \frac{3k + 1}{k + 1} \cdot \frac{2k - 1}{n - 1} \cdot \frac{1}{(k + 1)(n - 1)} \]  

(8)

B. Algorithm Description

In this section, we proposed a new information publishing and retrieval algorithm of small world architecture for p2p networks for information advertising and discovery inside and outside of peer groups. Each peer groups had a leader peer which kept a consistent index about members in the same group, and each peer node maintained some information about the leader peer nodes, leader peer nodes kept a small number of long links to distant peer node. A semi-structured approach was presented to create long range links between groups, as well as to discover the local peer nodes that had specific external connections. And the algorithm was described as follows:

Step 1 whether the initial peer node and the destination peer node was in the same peer group, if it was, then turned to step 2; else turned to step 4;

Step 2 the initial peer sent an advertisement, and pushed the advertisement to a target peer node according to the hash value of the name of the file, as well as the neighbors of the target peer node within a specific distance d to increase the probability of discovery of the advertisement. Then turned to step 3;

Step 3 the requesting peer node searched the target peer nodes generated from the same hash function, if the requested advertisement could not be found in the target node, the requesting peer node would continue to search the neighbors of the target peer node within a distance d, the program would be over until the advertisement was found, else turned to step 6;

Step 4 the initial peer sent an advertisement to the leader peer node, and the leader peer node pushed the advertisement to a target peer node according to the hash value of the name of the file, as well as other leader peer nodes which were neighbors of the target leader peer node within a distance d, turned to step 5;

Step 5 each leader peer nodes which got the advertisement sent the advertisement to a target peer node in the inter peer group according the hash value of the name of the file, and the neighbors of the target peer node within a distance d, turned to step 6;

Step 6 the requesting peer node sent the request to the leader peer node, and the leader peer node sent the request to a target leader peer node according to the hash value of the name of the file, and the requester peer node within a distance d away from target leader peer node, then turned to step 3.

IV. THE FRANGIBILITY OF PEER-TO-PEER NETWORKS BASE ON SMALL WORLD ARCHITECTURE

A simple small world architecture for P2P networks topology was illustrated in Figure 1. There were a lot of groups in the networks, the groups linked randomly, and every peer nodes in inter-group could communicate with each other freely, but the peer nodes in different groups should via leader peer nodes to communicate.

In order to compute the size of cluster when the ratio f of attack reached critical value, we may think as follows: after the ratio f of attack reached critical value, the network was broken up into clusters; the breakage was achieved by throwing off nodes. So in reverse, we looked at the progress for building networks by adding nodes, first, a network started by a single node, along with the join of other nodes and edges, there would be clusters had the same size of clusters that the network broken down when the ratio f of attack reached critical value. So we could analyze the size of cluster before the network would work. Assumed we randomly chose an edge, and along the edge pointed to an end node, through the end node, all the nodes could communicate smoothly, and we called the set of these nodes cluster. And we supposed the generated function of the cluster was \( G_i(x) \), so along the chose edge, the size of these clusters could be denoted by \( G_i(x) \). Also through an edge pointed to a node, the distribution of generated function of edges which linked to the node could be expressed as follows:

\[ \Phi_i(x) = \sum_{k=0}^{\infty} q_k x^k = \frac{\sum_{k=0}^{\infty} (k + 1) p_{k+1} x^k}{\sum_{j} j p_j} \]

\[ = \frac{\sum_{k=0}^{\infty} k p_k x^{k-1}}{\sum_{j} j p_j} = \frac{\Phi_i(x)}{z}. \]  

(9)
Where $q_k$ was the probability distribution of edges, these edge linked to a node, and through a randomly chose edge could visit to the node. According to the property of generated function, $q_k$ identified a $k$-linked clusters, and the distribution function of $k$-linked clusters was $[G_i(x)]^k$. So the number of nodes through a randomly chose edge could visit to that was generated by the following function:

$$G_i(x) = \sum_{k=0}^{\infty} q_k [G_i(x)]^k = x \Phi_i(G_i(x))$$ \hspace{1cm} (10)

We thought about a node, and supposed its degree distribution was $p_k$, because it maybe link to other clusters and the size of clusters was decided by generated function $G_i(x)$, so the size of cluster which the node maybe belong to could be expressed by the following generated function:

$$G_i(x) = \sum_{k=0}^{\infty} p_k [G_i(x)]^k = x \Phi_i(G_i(x))$$ \hspace{1cm} (11)

It was very difficult to compute $G_i(x)$ from formulas (10) and (11), but we could get a solution about $x$ in finites power series through iterative method of formula (10). Assumed we knew a similar solution of $\Phi_i(x)$, so put this solution into formula (10), and we would get a new solution. For example, in ER model, its degree distribution obeyed Poisson distribution and $\Phi_i(x) = e^{-x} + O(x^2)$, so put these formulas into formula (10), we got the following results:

$$zG_i^{(1)}(x) = xze^{-z} + O(x^2)$$
$$zG_i^{(2)}(x) = xze^{-z} + (xze^{-z})^2 + O(x^3)$$
$$\vdots$$
$$zG_i^{(5)}(x) = xze^{-z} + (xze^{-z})^2 + \frac{3}{2}(xze^{-z})^3 + \frac{5}{3}(xze^{-z})^4 + \frac{8}{3}(xze^{-z})^5 + O(x^6)$$ \hspace{1cm} (12)

From formula (12) we knew, if we randomly chosen a node, the probability distribution $P_s$ of the cluster which the node maybe belong to was:

$$P_1 = e^{-z}, \quad P_2 = ze^{-2z}$$
$$P_3 = \frac{3}{2}z^2e^{-3z}, \quad P_4 = \frac{5}{3}z^3e^{-4z}$$
$$P_5 = \frac{8}{3}z^4e^{-5z}$$ \hspace{1cm} (13)

From above formula (13), we knew it difficult to compute the solution of probability distribution $P_s$, but we could get its expectation value, that was the average size of clusters when the expectation value in rank 1. So we got the average size of clusters $s$

$$s = \frac{\Phi_i(G_i(x))}{1 - \Phi_i(G_i(x))}$$ \hspace{1cm} (14)

In formula (14), if $x=1$, then the value of generated function was 1 and $\Phi_i(G_i(1)) = 1$.

We got the differential coefficient of formula (10)

$$G_i'(1) = \frac{1}{1 - \Phi_i(G_i(1))}$$ \hspace{1cm} (15)

Based on the above formulas (14) and (15), we got the following results:

$$\sum_{s=1}^{\infty} \Phi_i(s) = \frac{1}{1 - \Phi_i(G_i(1))}$$ \hspace{1cm} (16)

And we knew that:

$$z_1 = \Phi_i(G_i(1)) = \frac{1 - N^{(2-\gamma)\gamma}}{\gamma - 2}$$ \hspace{1cm} (17)

$$z_2 = \Phi_i(G_i(1)) = \frac{N^{(3-\gamma)\gamma}}{3 - \gamma}$$ \hspace{1cm} (18)

So from the formula (11), we could compute the average size of clusters before the network work, which was to say, when the ratio of attack reached critical value, the average size of clusters was also $s$.

V. SIMULATION RESULTS

A. A small World Architecture For Peer-to-peer Networks

In this section we first studied the clustering coefficient and average path length of small world architecture for p2p networks topology in static environments. We assumed each peer node had identity number and some information, the leader peer node had an index of nodes in the same group and information, the number of peer nodes in each groups was 8, and the leader peer nodes was the one whose identity number could be divide by 8. We compared the clustering coefficient between small world architecture and random networks, and also compared the average path length among small world architecture, chord networks and...
random networks. The small world architecture for p2p networks had bigger clustering coefficient and shorter average path length.

We knew that the small world networks had two different characters from other networks those were bigger clustering coefficient and shorter average path length. So we compared the clustering coefficient between the small world architecture for p2p networks and random networks. From Figure 2, we knew that the clustering coefficient of small world architecture for p2p networks firstly neared 1, then as the number of peer nodes grew, it decreased a little, but it stopped decrease at last; The clustering coefficient of random networks was smaller, and as the number of peer nodes grew, it neared 0. We also compared the average path length among small world architecture for p2p networks, chord networks and random networks. From Figure 3, we knew that the average path length of random networks was longer and it keep still; the average path length of chord networks was long and it grew slowly as the number of peer nodes grew; and the average path length of small world architecture for p2p networks was the shortest. So the small world architecture for p2p networks had the same characters as small world networks.

We also studied the performance and the average time of successful search of small world architecture for p2p networks in static environments and dynamic environments. Figure 4 showed the average time of successful search both in static environments and dynamic environments. In static environments, the peer nodes found information easily, and the average time of successful search would decrease as the number of peer node grew; in dynamic environments, the peer node lost links frequently, so it took more average time of successful search and sometimes the average time of successful search would be abnormal. Overall, the small world architecture for p2p networks performed very well to search information.

B. The Frangibility For Peer-to-peer Networks

In this section we would present simulation results for the frangibility of p2p networks base on small world architecture. We assumed that the p2p networks had N nodes; the ratio of attack nodes was f. In experiments, we used three ways to remove the nodes, which were random failure, degree attack and betweenness attack. After the remove of the nodes, we detected the topology of p2p networks base on maximal clusters, centricity and diameter, and found out that when we removed the nodes base on degree attack, the super nodes would easily be cracked and the networks also would easily be destroyed into small pieces, for example, in Gnutella networks, there was about 3.3% super nodes, so if the ratio f of attacked nodes reached 4%, the Gnutella networks could never work. It is very important to protect the super nodes for controlling Gnutella networks. Compared with ER model, SWAN networks had different effect under different ways of attack, so we should take different strategies to control SWAN networks under different environment.
We knew that the ER model was put forward by mathematician Erdős and Renyi, and the ER model was characterized by its robustness to random failure and also frangibility to hostility attack. Figure 6 showed the maximal clusters of ER model under degree attack, betweenness attack and random failure, the three curves were almost overlay. That was to say, the different ways of attack had no distinctness effect of ER model. Figure 5 showed the maximal clusters of SWAN networks under different attack. For degree attack, when the ratio of removed nodes $f$ went to 2%, the maximal clusters went to zero, that was to say, the networks would not work; for betweenness attack, the ratio of removed nodes $f$ went to 3.3% until the network stop working.

Figure 7 and 8 showed the effect of diameter under different ways of attack. From 7, we knew that as the ratio $f$ increased, the diameter also increased rapidly under degree attack and betweenness attack, it told when the ratio of removed nodes $f$ went to 0.2%, the diameter of SWAN networks would not be controlled, except the random failure. Different from 7, the ER model had better resistance; the diameter of ER model could be controlled until the ratio of removed nodes $f$ goes to 5%.

Figure 9 and 10 showed the effect of centricity under different ways of attack. According to Figs 9, for degree attack, when the ratio of removed nodes $f$ went to 1%, the SWAN network had the minimal value of centricity 0.14; for betweenness attack, when $f$ went to 3%, the SWAN network also had a minimal value of centricity 0.15. We also found a strange phenomenon that the value of centricity grew bigger after it had reached the minimal value.

To sum up, the SWAN networks was robust to random failure and frangible to hostility attack, and according to the results of attack, the degree attack was most harmful, the second was betweenness attack. Different from SWAN networks, the ER model had similar effect but more frangibility.

VI. CONCLUSIONS

The small world phenomenon was well known and it greatly influenced the social and biological sciences. Due to the similarity between p2p networks and social networks, so we believed and confirmed that the small world phenomenon was also useful to improve p2p networks by constructing small world architecture. Frangibility is an import factor in the research of networks, and the study of frangibility of p2p networks base on small world architecture is also very necessary. So this paper presented a small world architecture for p2p networks. In such p2p networks, peer nodes freely linked to each other in inter-groups and not every peer node needed to be connected to remote
groups, and also could easily find the information in remote peer node via some leader peer nodes. It reduced the average distance and the lost of information and could achieve good performance in both static and dynamic environments. In this paper, we also gave a method to detect the topology of p2p networks, and also fully analyzed the fragility of Gnutella networks under degree attack, betweenness attack and random failure. The Gnutella networks were best fault tolerance when suffered randomly attack, but worst fault tolerance when suffered degree attack and betweenness attack. We also study the theory of fragility of p2p networks base on small world architecture and gave a closed-form solution for average size of clusters which before the largest cluster of networks had appeared. At last, we compared SWAN networks and ER model under different ways of attack. The next step we planed to further study the improvement of resistance to fragility and optimize the topology of small world architecture for p2p networks.

ACKNOWLEDGMENTS

This research was supported by the Natural Science Foundation of China (Grant No. 60673163).

REFERENCES


