ANALYZING THE P2P TRAFFIC USING PROBABILITY SCHEMES

M. Sadish Sendil[1] and Dr. N. Nagarajan[2]

[1] Research Scholar, Assistant Professor,
Department of Computer Science and Engineering,
SNS College of Technology, Sathy NH, Coimbatore, Tamilnadu, India
sadishsendil@yahoo.com
[2] Research Supervisor and Principal,
Coimbatore Institute of Information and Engineering Technology,
Coimbatore, Tamilnadu, India

ABSTRACT

Peer to Peer network has become one of the most important areas while sharing the information in the global world. When we can share the information in the p2p network, traffic is the major problem. We can analyze the traffic theoretically which are associated with broadcasting. For theoretical analysis, we propose and evaluate the probability based schemes like Uniform Probability, Dropped Probability, Dropped Message, Triangle Based and Biased Forwarded to alleviate traffic load on broadcasting networks. Reducing redundant traffic is a natural approach to alleviate the high traffic problem without compromising the reachability of messages. Some of the schemes can significantly reduce the whole network traffic with little or no cost on reachability and latency of messages. And also we proposed the multi-backup routing method that makes use of redundant traffic to enable more search results to reach a searcher.

KEYWORDS

P2P, UPBS, DPBS, DMBS, TBS, BFS

1. INTRODUCTION

Peer-to-peer (P2P) has become one of the most widely discussed terms in information technology. The term peer-to-peer refers to the concept that in a network of equals (peers) using appropriate information and communication systems, two or more individuals are able to spontaneously collaborate without necessarily needing central coordination. P2P networks promise improved scalability, lower cost of ownership, self-organized and decentralized coordination of previously underused or limited resources, greater fault tolerance, and better support for building ad hoc networks.

Nowadays research is going on in the broadcast techniques which are closely related to the context of wired networks. Most of them assume that broadcast plays an assistant role, and is employed to implement or improve unicast algorithms. For example, in wired networks, broadcastings are employed to carry control messages, to discover global network topology information used for unicast routing, and so on. In all these research, unicast, not broadcast, is the basic and principal method to deliver messages. They all assume that broadcast does not occur frequently. This is not the case in a broadcasting peer-to-peer network like the Gnutella network. In the Gnutella network, broadcast is the principal method to deliver messages between nodes, and it is implemented using flooding protocol, which operates on application layer. The dynamic property implies that any routing information collected by traditional unicast routing algorithms will be obsolete soon after they are collected, therefore traditional

unicast routing algorithms are not suitable in such an environment. Reducing redundant traffic is a natural approach to alleviate the high traffic problem without compromising the reachability of messages.

Based on Fred et.al, a cost-weighted graph *G* is constructed, where weights denote latency values on communication links. Transfer the packets from one node to another by using flooding operation. The performance of the proposed schemes can be measured by using simulator to simulate the whole network on which messages are broadcast utilizing those schemes. We measure a scheme's performance by comparing traffic load and average message reachability on the whole network realized under the scheme to that metrics realized under no scheme. To generalize our experiments, we adopted several network topologies of different sizes including three small world network topologies as well as the Gnutella network topology. The small world network topologies are generated based on a lattice in which each node is connecting to the nearest three neighbors clockwise. . From the literature of Y Huang, the following can be obtained and proved with the help of simulator.

For each network, we randomly assigned each node a latency parameter to simulate its computation power and connection speed. A smaller latency indicates a faster node. Latency parameters determine the order in which messages are processed. More specifically, when a message is forwarded from one node to another, it will carry a timestamp that is the time when the message is forwarded plus the average latency of the two nodes. Namely, the average latency of any two connected nodes is considered as the latency on the connection between them. For example, node X (with latency LX) forwards a message to node Y (with latency LY) at time t, after the message arrives at node Y, its timestamp will be t + (LX +LY)/2. The simulator always processes the message that has the smallest timestamp over the whole network. A network's latency assignment keeps unchanged for all experiments on the network. In our experiments, only broadcasting messages were simulated, and messages were never responded since we focused on how broadcasting affects traffic and how much traffic can be saved and how message reachability is impacted when utilizing those schemes. The Gnutella network topology was collected and assigned each node a random latency parameter to simulate its computation power and connection speed. We measured a scheme's performance on a run using the following two metrics.

Saved Traffic Ratio (ST)

The ratio was defined as the number of messages proliferated on the whole network under a scheme dividing by the number of messages proliferated on the whole network under no scheme.

Average Reachability (AR)

We measured a message's reachability by dividing the number of nodes reached by the message under a scheme by the number of nodes reached by the same message under no scheme. We averaged all messages' reachability to obtain the average reachability (AR) of a scheme.

2. PROBABILITY SCHEMES WITH RESULTS

2.1 UNIFORM PROBABILITY BASED SCHEME (UPBS)

An instinctive way to reduce traffic is to let nodes forward messages selectively. The selection can be done based on a threshold. This scheme adopts a uniform threshold ranging from 0 to 1. The value of the threshold determines the probability for a message to be forwarded. More specifically, when a node is ready to forward a message to a neighbor, it generates a random number between 0 and 1; only if the random number is less than or equal to the threshold, the node continues to forward the message to the neighbor. This process is repeated for each neighbor.

We present the results under this scheme with uniform probability 0.1 and 0.9 in Figure 1 and Figure 2. The results for other uniform probability are some kinds of intermediate states between these two. Other results show that when the uniform probability increases from 0.1 to 0.9, the two curves in Figure 1 move towards each other, then cross each other at some middle point, finally they reach the positions as shown in Figure 2. As we can see, under this scheme, the saved traffic ratio (ST) remains value around P whereas the average reachability (AR) keeps value around 1−P when TTL> 2.

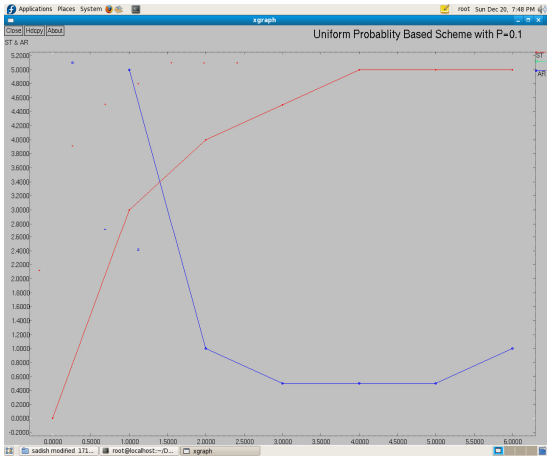

Figure 1. Uniform Probability Based Scheme with P = 0.1

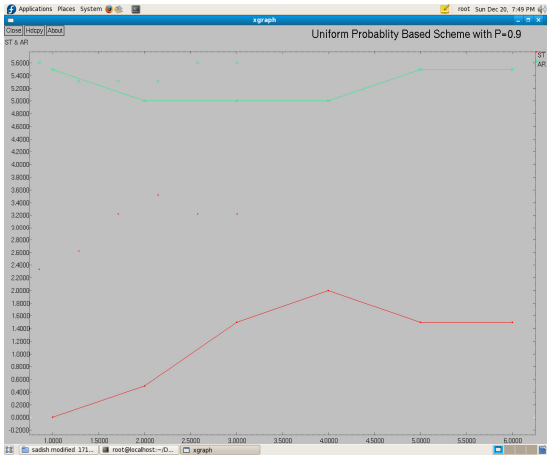

Figure 2. Uniform Probability Based Scheme with P = 0.9

2.2 DROPPED PROBABILITY BASED SCHEME (DPBS)

The Dropped Probability Based Scheme forwards the messages with probabilities varying with neighbors. Each node is having the information about the dropped messages of neighbor nodes. Using the count it checks whether a message is forwarded or not. If a node drops a message sent from a neighbor, the neighbor must drop the same message sent from the node. Based on the observation, the number of dropped messages from a neighbor could be an indicator of whether to forward subsequent messages to the neighbor or not. Instead of using the number directly, we use the ratio of the number divided by the number of total unique messages received at a node. Obviously the ratio ranges from 0 to 1. We call the ratio as the corresponding neighbor's dropped probability. In the DPBS scheme, when a node is ready to forward a message to a

neighbor, it generates a random number between 0 and 1; only if the number is greater than the neighbor's dropped probability, the node continues to forward the message to the neighbor.

The result in Figure 3 shows the average reachability (AR) keeps near 90% regardless of TTL. However, the saved traffic ratio (ST) is gradually increasing when TTL grows. Almost 40% traffic is saved at TTL=9. Note that the increasing is not unlimited but will stop after TTL goes beyond the diameter of the network.

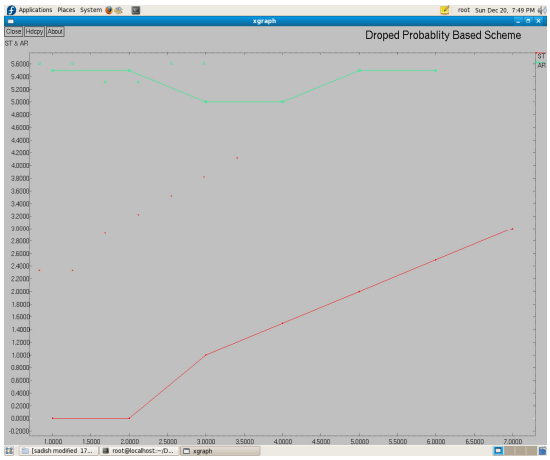

Figure 3. Dropped Probability Based Scheme

2.3 DROPPED MESSAGE BASED SCHEME (DMBS)

In this scheme, it is assumed that each message carries its originator's unique identifier. When a node drops a message from a neighbor due to duplicate, it associates the neighbor with the message's originator. Then later on when the node receives other messages from the same originator, it will not forward them to the associated neighbor any more. The idea is based on the fact that if an early message reached node X the first time without passing through node B, then subsequent messages from the same originator will reach node X the first time without going through node Y either. This happens when the transmission speed on each connection is stable on the network.

As described in the DPBS scheme, when a node drops a message from a neighbor due to duplicate, it gets to know that the neighbor drops its message too; it implies that the node is not on the shortest path from the originator of the dropped message to the neighbor. So the node should not send the neighbor messages that are from the same originator as the dropped message. Since the topology is dynamically changing, the associations should not be permanent. Another concern about this scheme is that there could be too many associations since there-exists a large number of nodes originating messages in the network. A solution is to keep a limited number of associations for each neighbor. The result in Figure 4 shows the average reachability (AR) remains around 100%. The saved traffic ration (ST) is increasing when TTL grows. Almost 60% traffic is saved at TTL=9.

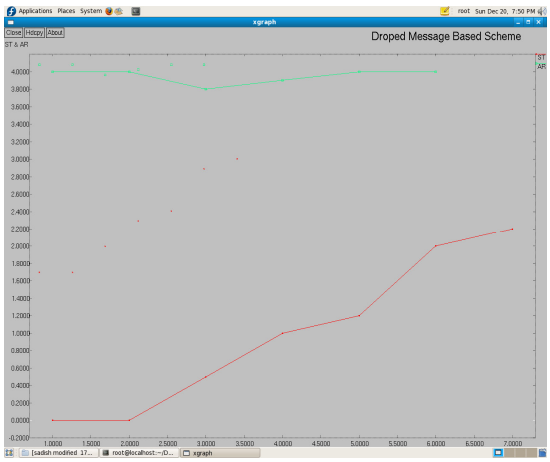

Figure 4. Dropped Message Based Scheme

2.4 TRIANGLE BASED SCHEME (TBS)

The triangle based (TBS) scheme is based on observation which follows: Assume node X, Y, and Z are pair wise connected therefore they establish a triangle sub network, when one of them broadcasts a message, the other two nodes do not need to forward each other the message since they can directly obtain the message from the first node. In TBS, each node needs to detect triangles in order to avoid redundant forwarding. A node detects triangle sub networks in the following way. When a node receives two messages that have three properties: (1) one message's hops value is one, another two; (2) they contain the same message identifier; and (3) they come from two different neighbors, then the node can be certain that it has established a triangle sub network with the two neighbors.

Once a triangle sub network is detected, any two of the three nodes can stop forwarding each other messages not only originated from but also passed by the third node. Since the topology is dynamically changing therefore a triangle sub network might be broken after detected, the detected triangle sub networks should have a limited period of lifetime. The result in Figure 5 shows the traffic load could be even worse (e.g. when TTL=2, 3) and was not significantly reduced under the TBS scheme. The Average Reachability (AR) remains around 100%.

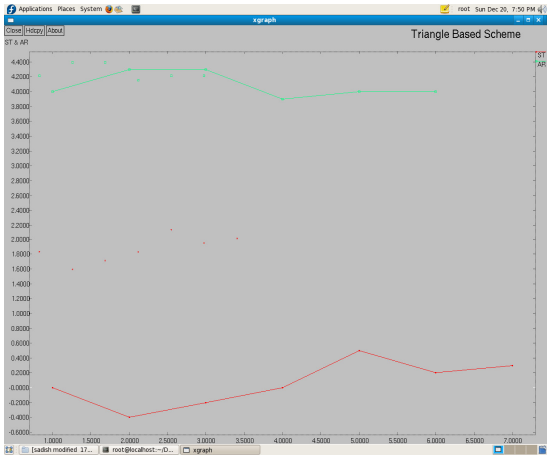

Figure 5. Triangle Based Scheme

2.5 BIASED FORWARDING SCHEME (BFS)

Compared to the UPBS, DPBS and DMBS this scheme works better in saved traffic ratio. But Average Reachability could be down to eighty percent. In the Biased Forwarding Scheme, nodes always forward messages to neighbors that have equal and lower or equal and higher degree if this forwarding is permitted by the flooding rule. The result under in Figure 6 shows the Saved Traffic (ST) and Average Reachability (AR) of the BFS. The above said schemes results are compared in the basis of Saved Traffic and Average Reachability. Figure 7 compares the Saved Traffic (ST), and Figure 8 compares the Average Reachability (AR) of the above said schemes.

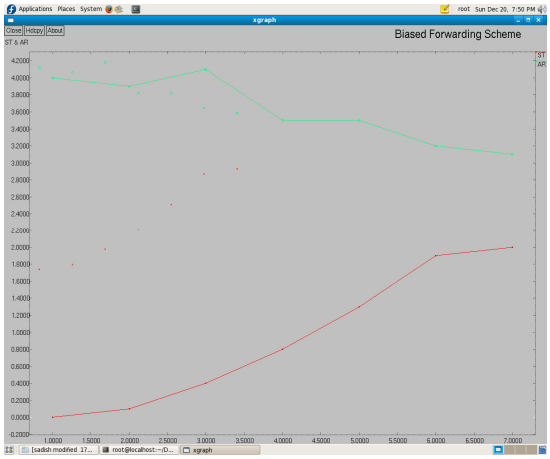

Figure 6. Biased Forwarding Scheme

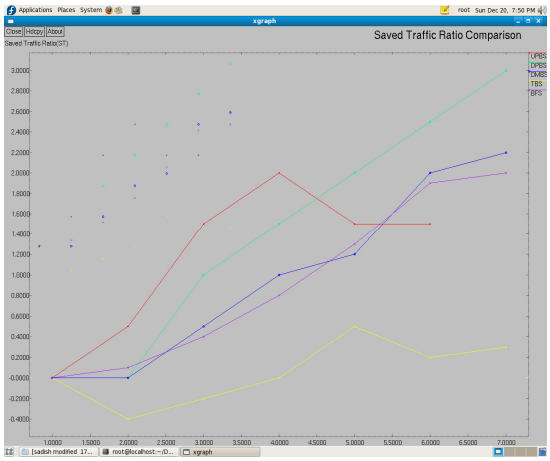

Figure 7. Comparison of Saved Traffic

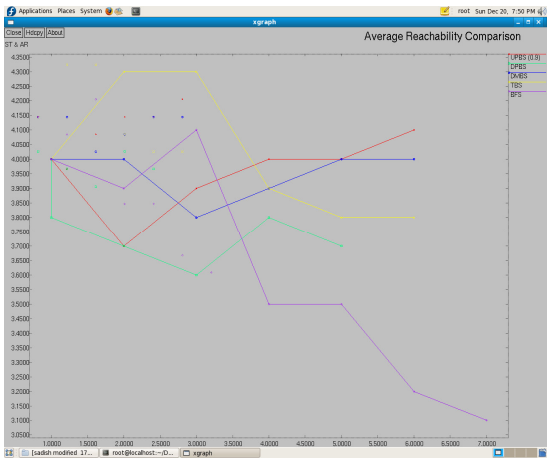

Figure 8. Comparison of Average Reachability

2.6 IMPROVING THE PERFORMANCE

Using the multi-backup routing, a node makes use of the duplicated copies of a message. When the replying messages come to the node, the node will choose and route the messages onto the first still-available connection in the same order. Figure 9 has shown how multi-backup routing works. Multi-backup routing improves the reliability for replying messages to reach their destination nodes. A little cost is that nodes have to record multiple (2 or 3, if there have that many) connections for each forwarded message. In Figure 9 (a), node X receives two copies of a message from two connections 1 and 2. The one from connection 1 comes earlier than another from connection 2, so node X forwards the first copy to node Y whereas drops the second one. In Figure 9 (b), node Y responds with a replying message to node X. Node X tries to forward the message onto connection 1, but it turns out that connection 1 has been broken, therefore node X forwards the message onto connection 2 other than drops the replying message as normal.

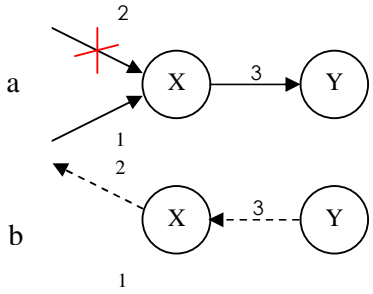

Figure 9. Comparison of Average Reachability

In the distributed file-sharing network, nodes can be from anywhere on the Internet. In many cases, nodes from within a private organization reside behind a firewall. They can make connection to the outside network, but cannot be connected to by others from outside the organization (i.e. outside the firewall). It implies that if a querying node outside the firewall is interested in a file offered by an offering node behind a firewall, the querying node possibly cannot actively download the file from the offering node, since the download connection cannot be established. In this situation, the two nodes can negotiate a push. That is, the querying node sends a message Push-Request to an outgoing neighbor of the offering node, in turn, the neighbor forwards the message to the offering node, and finally the offering node pushes the file to the querying node. Figure 10 depicts the relationship between these three nodes.

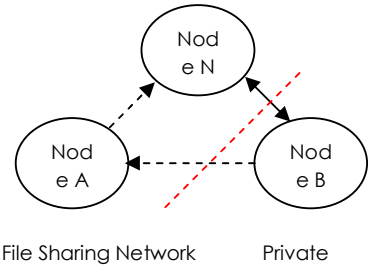

Figure 10. The Push Function in Firewall Environment

In Figure 10 node B sits behind a firewall within a private network and a firewall (square line) separates it from node A and node N. The solid line indicates the connection initiated by node B to its (outgoing) neighbor node N. When querying, node A requests node B to push a file, it creates a temporary connection and sends push-request to node N; in turn, node N forwards the request through the solid connection to node B; then node B creates an HTTP connection (dashed line) to node A and pushes over the file. In this case, neither node A nor node N can make connection to node B while node B can make connection to both of them. The performance can be improved by using the multi-backup routing and push method shown in the Figure 11 and 12 respectively.

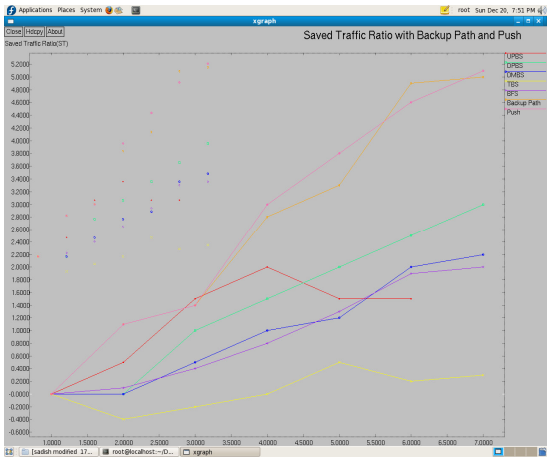

Figure 11. Comparison of Saved Traffic with Multi-backup and Push

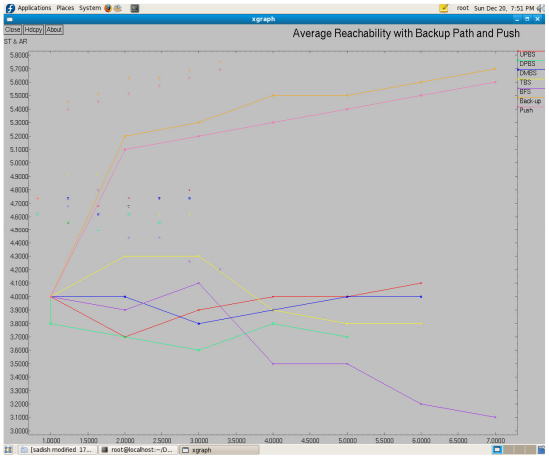

Figure 12. Comparison of Average Reachability with Multi-backup and Push

3. CONCLUSION

Here, we have shown the effect of broadcast on peer-to-peer networks, especially the effect on the Gnutella network. We have analyzed and addressed the traffic problem caused by broadcast on the Gnutella network and gave the solution using proposed five schemes to alleviate the traffic problem. And also we presented a multi-backup routing strategy to improve the reliability for replying messages to be routed back to corresponding requesting nodes by making use of duplicate messages. Using the multi-backup and push method, the traffic can be reduced. In future, we have to analyze how to reduce the duplication in the neighboring nodes using the feasible algorithm and methodology.

ACKNOWLEDGEMENT

The researcher would like to thank Dr. S.N. Subbramanian, Director cum Secretary, Dr. S. Rajalakshmi, Correspondent, SNS College of Technology, Coimbatore for their motivation and constant encouragement. The author would like to thank Dr. V.P. Arunachalam, Principal, SNS College of Technology for his valuable support to do the research. The author would like to thank Dr. N. Nagarajan, Research Supervisor and Principal, Coimbatore Institute of Engineering and Information Technology for critical review of this manuscript and for his valuable input and fruitful discussions. Also, he takes privilege in extending gratitude to his family members and friends who rendered their support throughout this research.

REFERENCES

[1] Angelo Spognardi, et al, (2005), A Methodology for P2P File-Sharing Traffic Detection, IEEE Proceedings of the Second International Workshop on Hot Topics in Peer-to-Peer Systems (HOT-P2P'05), 0-7695-2417-6/05

[2] Clay Shirky, (2000), What is p2p and what isn't, http://www.oreillynet.com/pub/a/p2p/2000/11/24/shirky1-whatisp2p.html

[3] Fred S. Annexstein, et al, (2001), Scalability Issues in Large Peer to Peer Networks – A case study of Gutella, http://citeseer.ist.psu.edu/cache/papers/cs2/580/http:zSzzSzwww.ececs.uc.eduzSz~annexstezSzPaperszSzscalabilityissues.pdf/jovanovic01scalability.pdf

[4] Fred S. Annexstein, et.al, (2001), Latency Effects on Reachability in Large-Scale Peer-to-Peer Networks, ACM ISBN 1-58113-409-6/01/07, pp 84-92.

[5] Gummadi K.P, et.al, (2003), Measurement, Modeling, and Analysis of a Peer-to-Peer File-Sharing Workload, in Proc. 19th ACM Symposium on Operating Systems Principles (SOSP-19), pp. 314-329.

[6] Lan Quan, et al, (2005), Performance Analysis of Unstructured Peer-to-Peer Schemes in Integrated Wired and Wireless Network Environments, IEEE Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05), 0-7695-2281-5/05.

[7] Li Jun, et.al, (2007), Active P2P Traffic Identification Technique, Proceedings of IEEE Computational Intelligence and Security, 0-7695-3072-9/07.

[9] Marcell Perenyi, et.al, (2006), Identification and Analysis of Peer-to-Peer Traffic, Journal of Communications, Vol. 1, No. 7.

[10] Sadish Sendil M, et al, (2009), An Optimized Method for Analyzing the Peer to Peer Traffic, European Journal of Scientific Research,Vol.34 No.4, pp.535-541.

[11] Sadish Sendil M, et al, (2009), Analyzing the Peer to Peer Traffic Aggregation Using an Optimized Method, Journal of Computer Science 5 (10): 738-744.

[12] Satoshi Ohzahata, et al, (2008), A Study on Traffic Characteristics Evaluation for a Pure P2P Application, IEEE 16th Euromicro Conference on Parallel, Distributed and Network-Based Processing, 0-7695-3089-3/08, pp 483-490.

[13] Subhabrata Sen, et al, (2004), Analyzing Peer-to-Peer Traffic Across Large Networks, in IEEE / ACM Transactions on Networking, Vol. 12, No. 2, pp 219-232.

[14] Xiaojun Hei, et.al, (2007), A Measurement Study of a Large-Scale P2P IPTV System, in IEEE Transactions on Multimedia, Vol. 9, No. 8, pp 1672-1687.

[15] Yunfei Zhang, et al, (2006), Recent Advances in Research on P2P networks, IEEE Proceedings of the Seventh International Conference on Parallel and Distributed Computing Applications and Technologies (PDCAT'06), 0-7695-2736-1/06.

Bibliography

M. Sadish Sendil received his M.E. degree and B.E., degree in Computer Science and Engineering from Anna University, Chennai and Bharathidasan University, Trichirappaly respectively. He is currently working towards the PhD degree in Computer Science and Engineering at ANNA University, Coimbatore. His research interests accumulate in the area of Reliability, Routing, and Network management in P2P Networks. He is a member of ISTE and Indian Computer Society.

Dr.N.Nagarajan received his B.Tech and M.E. degrees in Electronics Engineering at M.I.T Chennai. He received his PhD in faculty of information and communication engineering from Anna University, Chennai. He is currently working as Principal, Coimbatore Institute of Engineering and Information Technology, Coimbatore. He is member of board of study of faculty of information Technology at Anna University, Coimbatore. His specialization includes optical, wireless Adhoc and sensor networks. He is guiding assorted research scholars in optical networks and adhoc networks.