Reliable Peer Discovery in Content-Aware Overlay Network

Jayashree D
Research Scholar
Anna University
Chennai, Tamilnadu, India

Yogesh P
Associate aprofessor
Anna University
Chennai, Tamilnadu, India

ABSTRACT

Peer to peer (p2p) file sharing protocol and ad hoc wireless routing protocol shares many intriguing similarities even though they operate on a totally different level of a network. With the popularity of p2p application for resource sharing and the availability of resources has motivated the researchers to examine the potentials of p2p applications in a dynamic environment. With the success of p2p for file sharing applications, its benefits can be brought by constructing the overlay network with easy access of content to improve their availability and performance. This paper is one such an attempt to exploit the potential of mobile characteristics for the benefit of p2p application to satisfy the users demand. This paper focuses on how reliable content sharing could be realized in an ad hoc environment through peer to peer (p2p) system. This efficient content delivering system reduces the search latency of content peer selection. Also the reliable path for sharing content with trust calculation has been proposed. Unstructured peer to peer network is considered for the platform, emphasizing the content based interaction with a pro-active routing protocol at the network layer. The experiments have been performed on the network simulator NS-2 and the results showed that the proposed system improves the hit ratio and reduces the overhead traffic**.**

Keywords

Peer-to-Peer Network, Ad hoc network, Resource search, Trust.

1. INTRODUCTION

In the past few years, peer-to-peer systems (p2p) have become a major research topic as an efficient means for sharing data among autonomous nodes. The reason that made them one of the fastest growing Internet applications is that they offer the potential of low cost sharing of information, autonomy and privacy. However, finding a reliable peer for file-sharing applications is also one of the hurdle for accessing. With the increasing number of wireless and mobile devices, exploring the dynamic nature of the mobile environments for the benefits of p2p applications has been the driving force for research activities in this area. In p2p application, content sharing is an application task that allows devices of different capacities share their content to satisfy the users' needs in a distributed manner. In the absence of proper infrastructure the mobile devices are promising to share the content with an approach for pro-active searching and upgrading.

The content-based search methods are well suited for applications focused on content availability with a known set with bounded cost. In the face of the variety of peer-to-peer applications and services, the most noted operation is to locate the shared objects professionally, which are distributed among the nodes. The topology of the overlay network and placement of the data should be constructed with the communication properties of underlying layer in mind to reduce the search latency. It is better to form an overlay network for the distribution of the information among the peers rather than working with the underlying networks directly. One of the important challenges of these overlay network supported by mobile nodes is to provide content with less overhead find the reliable nodes. For both p2p overlay network and ad hoc network, the lack of coordination could easily lead to performance degradation.

Conventionally, mobile devices operate by locating the nearest available trusted wireless point in order to access a known wired backbone. However, despite advances being made in lean computing and power conservation on mobile devices, these resources remain constrained and often nodes in a network find it preferable to operate on low energy in order to access local services. Furthermore, addressing unreliability through repeating retransmissions in a low energy network wastes precious bandwidth. For the purpose of this paper, the trust model presented utilizes the success rate of networking requests as one of the criteria set for achieving quality of service. Investigating quality of service itself is outside the scope of this paper and will be presented in future work.

This paper investigates the behavior of the network with respect to entity feedback provided by peer request, and reflects the changing trust landscape.

The Gnutella, P2P file sharing protocol has been chosen from many unstructured P2P file sharing protocols (Napster and KaZaA are typical examples), because, it strikes a good balance between decentralization and scalability. Ad Hoc On-Demand Distance Vector protocol (AODV) protocol has been used for routing, other on-demand driven ad hoc routing protocols such as DSR could potentially be used as well.

The rest of the paper is organized as follows:

- Section II briefly presents the related work.
- Section III explains the proposed work
- Section IV reports the simulation results
- Section V concludes the paper.

2. RELATED WORK

The convergence of wireless technologies and peer to peer application allows seamless access to the Internet for mobile users. P2P systems have shown explosive growth in recent years, mainly due to their robustness, scalability, and availability. In unstructured peer-to-peer networks, to reduce the bandwidth requirement and to improve the efficiency of the flooding mechanism, selective search methods are used. Researchers have tried variations of classical search techniques, other than normal flooding: directed breadth first search (BFS) and iterative deepening [2], expanding ring [3], and random walk [4,5]. Biased search method sends messages only to the nodes that are more likely to get the information, instead of transmitting messages to all their neighbours. The methods used in [13,14,15] are sending messages only to the nodes that are more likely to get the information. It reduces the bandwidth consumption and streamlines the flooding method. In random walk [15] and dynamic query [16] the nodes are chosen by best path for transmitting and by using certain policy to select. [17,18, 19,20] used uniform index based caching or replication mechanisms to keep the known objects in the nodes on the transmitting path. [21] used adopted locality based multicast or routing algorithms of the application layer when constructing overlay networks. They draw the multicast using semantic approach. mOverlay network [22] is proposed to decrease the communication cost between nodes using the dynamic landmark technique to achieve the load balance and avoid the hotspots. A double-layered p2p system considering mobility for reliability in [9] has introduced the mobility based selection for sender peer. In [9] the author never consider the underlying layer locality to select the peer. Building on the observation that well matching overlay and underlay structures in MANETs imply less physical layer hops corresponding to virtual overlay hops, Mawji et al. [10] introduce a topology control algorithm to reduce energy consumption and response times. In [11] node connects to neighbors based on two heuristics, namely the remaining energy levels of peers and the physical layer distance to other peers. ORION [12] is one of the typical single-layered systems. In ORION, the communication is performed based on the flooding mechanism and each peer has a routing table and a file route table for routing. The main disadvantage of ORION is that network traffic may be increased rapidly when there are many peers within the communication range and a very large number of different files are distributed throughout the network. Recently, another approach to reduce energy consumption of peer-to-peer overlays built on top of mobile ad hoc networks and based on the theory of topology control has been proposed [10]. Improvements to this work included the introduction of peer mobility as an additional super-peer selection heuristic, as well as the modification of the IEEE 802.11 power saving mode in conjunction with the aforementioned two-layer p2p system to further decrease energy consumption.

Damiani et al [24] proposed XRep: a reputation-based approach for evaluating the reputation of peers through distributed polling algorithm before downloading any information. The approach adopts a binary rating system and it is based on GNutella [25] query broadcasting method using TTL limit. EigenTrust [26] collects the local trust values of all peers to calculate the global trust value of a given peer. Additionally, EigenTrust adopts a binary rating function, interpreted as positive one (representing satisfactory), or zero or negative one (representing unsatisfactory or complaint).Marti and Garcia-Molina [27] proposed a voting reputation system aiming at e-commerce applications that collects responses from other peers on a given peer. The final reputation value is calculated combining the values returned by responding peers and the requesting peer's experience with the given peer. This seems more reasonable than the model in the work by Damiani et al [24]. However, this work and the work by Kamvar et al. [26] did not explicitly distinguish transaction reputation and recommendation reputation. This may cause severe bias in reputation evaluation as a peer with good transaction reputation may have a bad recommendation reputation especially when recommending competitors

Wang and Varadharajan [28] proposed several trust metrics for the trust evaluation in a decentralized environment (e.g., P2P network), where a trust value is a probabilistic value in the scope of [0, 1]. Prior to the interaction with an unknown Peer Px, the end-peer collects other peers' trust evaluations over Px. A method has been proposed for trust modification after a series of interactions with Px that a good value results from the accumulation of constant good behavior leading to a series of constant good trust values. In another work by Wang and Varadharajan [23], the temporal dimension is taken into account in the trust evaluation wherein fresh interactions are weighted more than old ones

This paper provides a specific method to reduce the search delay and present a maximum reliable transmission for resources. This paper presents a method for Gnutella, an open and widely used system to provide content based search on the application layer. The key idea is to simplify the search by grouping under application of multicasting algorithm and enables a smarter overlay construction. These features come at the expense of unique group formation with required multicast activity. In order to provide content search and access the reliable peers these groups are form the overlay network and calculate the reliability based on their positive transaction.

3. PROPOSED WORK

P2P paradigm is particularly suited to enable content distribution, communication and collaboration applications in the dynamic environment. Tolerance to the dynamic nature of the nodes, open platform like Gnutella distributes data without the need for centralized servers. To enable peer applications in mobile background, peers have to organize themselves as logical overlay network and provide reliable communication. The most important advantage of the Gnutella architecture is its independence of central servers, and other advantages like cost-effectiveness, fault tolerance and ability to work without maintenance becomes possible. However, since the Gnutella protocol is based on propagating broadcast messages, it stresses more on networks. The amount of transferring broadcast messages in ad hoc network increases exponentially with a linear increase of the depth of the search. For further development of P2P towards the mobile world, two possible modifications have been implemented. First one is a more generic approach develops a resource oriented accessibility system with minimum search time that would selectively position the resources in the P2P overlay. This method devise a stable resource accessing scheme for mobile devices that can reduce the transmission overhead and accessing time.

For the first alteration the peers are framed into groups within the overlay network based on the content types available with the network. Each content type forms a group which runs any multicast algorithm for control messages within that group. For a peer join phase, modified ping / pong messages have been used to establish the connection to any number of groups.

In this paper, the second modification proposed is a trust mechanism that includes both trust calculation and finding shortest trust path. It allows a realistic operation of Peer-to-Peer services over ad hoc networks. It spans from the network layer and tries to reuse existing protocols as far as possible. Additionally the network layer needs knowledge about the trustworthiness of these peers. Providing a trusted path for resource sharing can help the peers to obtain trustworthy acquaintance of neighbors without the fear of losing the packets to malicious peers.

3.1 Content Aware Group Formation

Gnutella runs on application layer on the existence of an unstructured overlay network. Gnutella specification assumes that each peer is given a boot-server as an entry point in the overlay. Bootstrap peer helps each peer to establish connections in the overlay network.

In our research work, locating neighbour's peer process relies on a node called the Maintenance Node (MN) that has information of all the bootstrap (BS) peers in the overlay network. When a node joins the overlay network, its first reaches the MN and gets the address of the bootstrapping peer randomly. The process of identifying bootstrap peer has been adopted from mOverlay network searching algorithm [8], which randomly provides the bootstrapping hosts in order to balance the load of the nodes in the network. Here the bootstrap peer would contain a number of peergroups' Gateway_peer (GWP) the one through which any peer has to join its content group. Each peer tries to establish connection to the group according to the type of contents it wants to share. The bootstrap peer identifies the requested content type of the joining peer 'i' and replies back with the address of the known Gateway_peer of that requested peer group. The peer 'i' after receiving the address of the Gateway_peer a ping message to that Gateway_peer The peer 'i' has received more than one address of the Gateway_peer for the same content type, the shortest distance in the under-laying network would be markedly as the Gateway_peer for that group. In this way, a peer becomes the member of the content multicast group. Peer proactively open minimum amount of connection and accept the incoming connection according to the upper bound limit for the number of links to open. The lower bound has been fixed as 2 and upper bound as 10 to make any peer to be part of min 2 groups to maximum in 10 groups.

In this paper, groups are composed of peers with the same resource type. In later periods if a peer wants a particular content, a search process is initiated to find the Gateway_peer for that group. If the peer could not find Gateway_peer the locating process initiates a search procedure iteratively. The ping process is initiated. This ping process may terminate after a fixed number of trials. In our simulation, 5 is the upper bound limit. The node will form a new resource group, if the locating procedure hasn't found the required resource group over 5 times for the retransmission of ping process.

After first connection the peer discovers other nodes by issuing ping messages. Peers receiving a valid pong message containing their content type along with the normal Gnutella pong attribute. Peers replay back, through the path followed by the ping messages. Each pong message can be cached on the way back to ping message creator. The caching reduces the content discovery overhead.

Using the above mechanism the content aware groups are formed. In these content aware groups, connections are established directly between the requestor and the Gateway_peer to start the file search on that group. This avoids the necessity for the requester to go for a linear search rather the requestor peer gets the information on the content aware group from the Gateway_peer. This reduces the message overhead and saves bandwidth and have our system leads the P2P system with enhanced scalability.

As the peer starts its search it looks for the content into its content table for the Gateway_peer. If the peer has the content group's Gateway_peer the request is sent to that peer. Since that is entry part of that content group the spread would start from there. From there that peer would circulate the query to the Group through multicast communication. This way the query message has been restricted to that particular group In this way the search has limited to some set of content group and search time has been reduced.

If that content Gateway_peer is not available it will spread to its neighbours to get hold of any of their Gateway_peer of that content group. The neighbours pass that request to that Gateway_peer and send that info back to the requested peer with the Gateway_peer ID and that requested peer send a direct request to that Gateway_peer.

In our method Query and QueryHit have slight variation comparing the existing Gnutella. On receiving the query message a peer look locally stored content to find the exact match of the content requested in the query message. The peer will send back the queryhit message if the match has been found. The following attributes are added to the existing Query and QueryHit messages. After receiving the query from any peer Gateway_peer look up for that content availability.

3.2 Reliable Peer

In a Mobile P2P network, some peers join or leave the network frequently, which leads to the dynamic topology changes. As a result, a trust management system needs to frequently update trust ratings, which in turn can increase the communication overhead. The presented proposal can easily adopt by any routing algorithm without much overhead to find a trusted path.

Path trust is the trust value associated with the path. This value is defined as the weighted average of the trust values of the nodes in the path. As trust is considered to be, asymmetric mutual trust between the nodes is used. Hop count also plays a prominent role in the selection of the path since the larger the number of nodes, more is the delay in the network and chances of information modification also increases. To search for trusted data provider EDSR offers a similar message like the Gnutella query-message. At the end of each message, the current node stores its own IP address and the trusted value of the next hop peer. Thus, the route of the reply message is predetermined.

Request packet: Request packet header is modified by adding an F-trust value. Hence, that it now contains the following fields: source IP address, destination IP address, a sequence number and F-trust. Each broadcast packet is modified to include the trust value of the node from which packet is received. So when Source a broadcasts a request packet and node B receives it, it updates the F-trust (forward trust) value such as

$$F_{trust} = F_{trust} + {}_{A}T^{B}(\text{trust value of A for B}) \quad (1)$$

At the destination, F-trust contains information about the trust of all nodes involved in the path.

Reply Packet: Reply packet is modified to accommodate the F_{trust} and B_{trust} values. Each node updates it by including the trust value of the node from which it received the packet. So when node X receives reply from node Y, it updates B-trust as:

$$B_{trust} = B_{trust} + {}_{X}T^{Y}\,(\text{trust value of X for Y}) \quad (2)$$

When the Reply packet reaches the source node, the most secure path is selected by it. It calculates the path trust based on the trust values F-trust and B-trust received in the Reply packet and the number of nodes in the path. The path selected is the one, which has the maximum path trust.

Trust value of i^{th} path is:

$$\text{Trust Path value} = \left[\left(F_{trust} + B_{trust}\right)/2\right] * W_{t_I} \quad (2)$$

Where Wt of i^{th} path is

$$W_{t_i} = \frac{\left[\dfrac{1}{\text{no of nodes in the } i th \text{ path}}\right]}{\displaystyle\sum_{i=1}^{n} \frac{1}{\text{no of nodes in } i th \text{ path}}} \quad (3)$$

n is the total number of path discovered from s to d.

Wt_i is the weight assigned to the i^{th} path.

Trust path value is the trust value of the path selected as the most trust-worthy path. As in the case of search requests, the structure of a reply is based on the structure of a ROUTE REPLY (RREP) of EDSR. Additionally it holds the transmitting peer id, destination peer id and the trust value for the next hop peer. Otherwise, all the other packet details have been maintained along with their trust value.

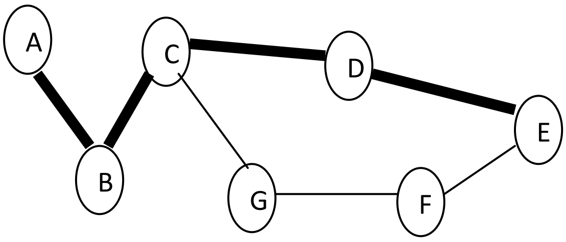

Fig 1: Path Trust Calculation from peer A to E

The above network model explains the Path Trust value calculation from node A to E through nodes A, B, C, D, and E.

$$\text{Trust value path}_{A-E} = \left[\frac{\left({}_{A}T^{B} + {}_{B}T^{C} + {}_{C}T^{D} + {}_{D}T^{E} + {}_{E}T^{D} + {}_{D}T^{C} + {}_{C}T^{B} + {}_{B}T^{A}\right)}{2}\right] * W_{t_i} \quad (4)$$

Trust Path from A to E contains mutual trust information of all the nodes involved in the path from A to E.

4. PERFORMANCE EVALUATION

In this paper, the network simulator NS v2.34 [22] for the experiments has been used. Nodes in the simulation, moved according to random waypoint model. Random waypoint model defines the mobility pattern of nodes by the pause time and the maximum node speed. Each node began the simulation by remaining stationary for the specified pause time. It then selected a random destination in the given space and moved to that destination at a speed distributed uniformly between 0 and 5 m/s speed. Upon reaching the destination, the node paused again for the pause time, selected another destination, and proceeded from there as previously described. To simulate the trust path calculation in a mobile ad-hoc network environment, NS2 v2.28, a network simulation tool, is used. EDSR protocol is adopted as a routing protocol, with 1500m1500m in the size of network area. The simulation is carried out with a change in the number of peers ranging from 20 up to 100.

.

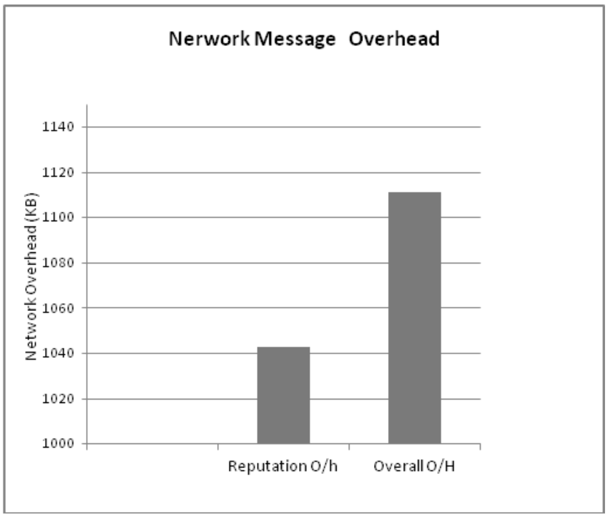

Fig 2: Overhead for reputation calculation and overall

fig 2 shows reputation calculation overhead and overall network overhead for each system. Here overall overhead comprisis of the control messages for network formation, the messages sent for finding the resources through queries and for calculating trust. The trust overhead for proposed method occupies 21.3 % of overall overhead. The group formation reduces the search hence the query overhead reduction.

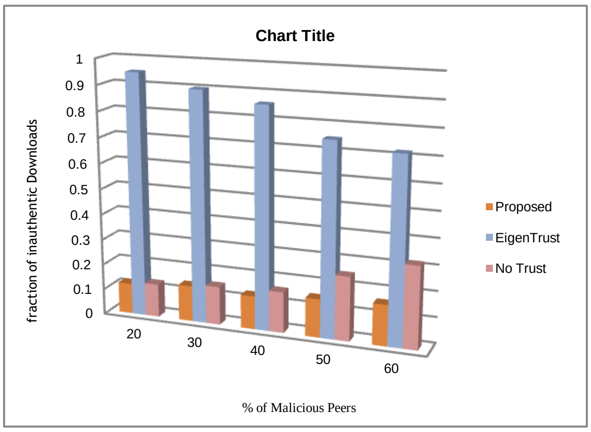

Fig 3 **Trust-**based reduction of inauthentic downloads in a network where a fraction of peers forms a malicious collective and always uploads inauthentic files.

Forming a malicious collective does not boost the trust values of malicious peers significantly, they are still virtually banned from uploading inauthentic files. For the figure 3, experiments are run on a system where download sources are selected based on our global trust values and on a system where download sources are chosen randomly from the set of peers responding to a query.

The proposed system performs well even if the malicious peers' percentage is increased. The experiment clearly shows that forming a malicious collective does not decisively boost the global trust values of malicious peers: These peers are tagged with a low trust value and thus rarely chosen as download source. Under the presence of pre-trusted calculated values, the local trust values of malicious peers are significantly lower than those of good peers already after one simulation cycle. This minimizes the number of inauthentic downloads. For example, with 60% of peers in a network being malicious, around 84% of all file downloads will end up in down - loading an inauthentic version of the file in a normal, non-trusted method. Our proposed method shows 22% lesser downloading proportion from Eigentrust model [25]. It shows the method of normalizing has played a heavy role in computing trust values and that alone make the rise in inauthentic download.

5. CONCLUSION

This paper presents a novel method of finding resources and the most trusted path for obtaining the resource for a mobile peer. The formation helps to narrow down the search and reduce the overhead. The trust relies on direct trust ratings and witness recommendations from reliable peers to determine trust ratings for a node using confidence value. Simulation results demonstrate that the overall performance of this scheme is reliable and have marginal increment in their overheads for detecting trusted peers in P2P mobile networks.

In the future, we should do more work to research the discrimination of the malicious actions and deploy the framework in a real system. More detailed simulations that consider the dynamic nature of the network where the protocol is to be deployed, and with a more sophisticated modelling of the attackers according to the network's possible vulnerabilities, would be needed to get a more realistic evaluation of the proposed architecture for deployment in an actual system.

6. REFERENCES

[1] Mascolo. C, Capra. L, and Emmerich. W. (2002) 'Middleware for Mobile Computing (A Survey)' In E. Gregori, G. Anastasi, and S. Basagni, editors, Neworking 2002 Tutorial Papers, LNCS 2497, pages 20–58.

[2] Yang. B, and Garcia-Molina H, (2002) 'Efficient search in peer-to-peer networks', Proceedings of the 22nd International Conference on Distributed Computing Systems, July.

[3] Lv, Q., Cao, P., Cohen, E., Li, K., and Shenker, S., (2002) 'Search and replication in unstructured peer-to-peer networks', in ICS '02 : Proceedings of the 16th International Conference on supercomputing, June.

[4] Adamic, L., Lukose, R.M., Puniyani, A.R. and Huberman, B.A., (2001)'Search in power-law networks', Physics Review Letters, no. 64 046135.

[5] Lv, Q., Ratnasamy, S., and Shenker, S., (2002) 'Can heterogeneity make gnutella scalable?' in IPTPS '02: Proceedings of the 1st International Workshop on Peer-to-Peer Systems.

[6] Lv, Q., Cao, P., Cohen, E., Li, K., and Shenker, S., Search and replication in unstructured peer-to-peer networks," in Proceedings of the 16th International Conference on supercomputing (ICS '02), June 2002.

[7] Klingberg, T., Manfredi, R., (2002)' Gnutella 0.6'[Online], http://rfc-gnutella.sourceforge.net/src/rfc-0_6-draft.html.

[8] Zhang, X. Y., Zhang, Q., Zhang, Z., Song, G., and Zhu,W., (2004), 'A Construction of Locality-Aware Overlay Network: mOverlay and Its Performance,' IEEE Journal Selected Areas in Communications Vol.22, No. 1, pp. 18-28.

[9] Kim, S.K., Lee, K.J., and Yang, S.B., (2011) 'An Enhanced Super-Peer System Considering Mobility and Energy in Mobile Environments,' in ISWPC-11: Proceedings of 6th International Symposium on Wireless and Pervasive Computing.

[10] Mawji, A., Hassanein, H., and Zhang, X., (2011) 'Peer-to-peer overlay topology control for mobile ad hoc networks', Pervasive and Mobile Computing, Elsevier, vol. 7, no. 4. pp. 467-478

[11] Rao, W., Chen, L., Wai-Chee Fu, A. and Wang, G., (2010) 'Optimal Resource Placement in Structured Peer-to-Peer Networks', IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 7, pp. 1011 - 1026

[12] Schollmeier, R., Gruber, I., and Niethammer, F., (2003) 'Protocol for peer-to-peer networking in mobile environments, in ICCCN 2003: Proceedings of the 12th International Conference on Computer Communications and Networks, pp. 121–127.

[13] Yang, B., and Garcia-Molina, H., (2002) 'Efficient Search in Peer-to-Peer Networks,' Proceedings International Conference on Distributed Computing Systems, Vienna, Austria, pp. 5-15.

[14] Ratnasamy, S., Handley, M., Karp, R., and Shenker, S., (2002), 'Topologically-aware Overlay Construction and Server Selection,' INFOCOM 2002: Proceedings of the Twenty-First Annual Joint Conference of the IEEE

Computer and Communications Societies. IEEE, New York, NY USA, vol. 3, pp. 1190-1199

[15] Lv, Q., Ratnasamy, S., Shenker, S., (2002), ‘Can Heterogeneity Make Gnutella Scalable?’ The First International Workshop on Peer-to-Peer Systems, Springer-Verlag, Cambridge, MA, USA, pp. 94103.

[16] Z., Tang, C., and Zhang, Z., (2003), ‘Building Topology-Aware Overlays Using Global Soft-State,’ Proceedings of the 23rd International Conference on Distributed Computing Systems, IEEE, Providence, Rhode Island USA, pp. 500-508

[17] Chen, W. -T., Chao, C. -H., and Chiang, J. -L., 2006, “An Interest-Based Architecture for Peer-to-Peer Network Systems,” Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA’06), Vienna, Austria, Vol. 1, pp. 707-712.

[18] Wang, J. Z., and Vanninen, M. A., 2004, “A Novel Self-Configuration Mechanism for Heterogeneous P2P Networks,” Proceedings of IEEE/WIC/ACM International Conference the Intelligent Agent Technology, IEEE, Beijing, China, pp. 281-287.

[19] Bestavros, A., and Jin, S., 2003, “OSMOSIS: Scalable Delivery of Real-Time Streaming Media in Ad-Hoc Overlay Networks,” Proceedings of the 23rd International Conference on Distributed Computing Systems Workshops, IEEE Computer Society, Vienna, Austria, pp. 214-219.

[20] Cohen, E., and Shenker, S., 2002, “Replication Strategies in Unstructured Peer-to-Peer Networks,” SIGCOMM Computer Communication Review, Vol. 32 No. 4, pp. 177-190.

[21] Sun, Y., Sun, L., Huang, X., and Lin, Y., 2006, “Resource Discovery in Locality-Aware Group-Based Semantic Overlay of Peer-to-Peer Networks,” Proceedings of the 1st International Conference on Scalable Information Systems, ACM, Hong Kong, Article No. 44.

[22] Zhang, X. Y., Zhang, Q., Zhang, Z., Song, G., and Zhu, W., 2004, “A Construction of Locality-Aware Overlay Network: mOverlay and Its Performance,” IEEE Journal Selected Areas in Communications, Vol. 22, No. 1, pp. 18-28.

[23] Dou Wen, Wang Huaimin, Jia Yan , et al (2004) A recommendation-based peer-to-peer trust model [J]. Journal of Software,15(4): 571-583,

[24] GNutella.http://www.GNutella.com/.

[25] SD. Kamvar, M. T. Schlosser, and H. Garcia-Molina., (2003) The eigentrust algorithm for reputation management in p2p networks. In Proceedings of the 12th International WWW Conference, Budapest, Hungary, May.

[26] S. Marti and H. Garcia-Molina, (2004) “Limited reputation sharing in p2p systems,” Proceedings of ACM EC’04, New York, USA, pp 91– 101, May.

[27] Y. Wang and V. Varadharajan. Interaction trust evaluation in decentralized environments. (2004) In K. Bauknecht, M. Bichler, and B. Pr¨oll, editors, Proceedings of 5th International Conference on Electronic Commerce and Web Technologies (EC-Web04), volume LNCS 3182, Springer-Verlag, pages 144–153, Zaragoza, Spain, August-September.

[28] B. Yu, M. P. Singh, and K. Sycara. (2004) ,Developing trust in largescale peer-to-peer systems. In Proceedings of 2004 IEEE First Symposium on Multi-Agent Security and Survivability, pages 1–10, August.