PP-FSM: Peer to Peer File Share for Multimedia

Arsalan Ali Shah, Zafar I. Malik, and Shaukat Ali

Abstract— Peer-to-Peer (P2P) is a self-organizing resource sharing network with no centralized authority or infrastructure, which makes it unpredictable and vulnerable. In this paper, we propose architecture to make the peer-to-peer network more centralized, predictable, and safer to use by implementing trust and stopping free riding.

Keywords— File Share, Free Riding, Peer-to-Peer, Trust.

I. INTRODUCTION

The emergence of Peer-to-Peer (P2P) has opened a new dimension for file sharing application, such as Napster [1], Kazaa [2], and Gnutella [3]. P2P system is a global file share, storage and searching by using end to end nodes. The files shared on a P2P network are huge, their range is almost limitless, but we are limiting ourselves only to Multimedia Data. e.g. Picture, Audio, Video and Text. The Morpheus [4] multimedia file-sharing system reported over 470,000 users sharing a total of .36 petabytes of data as of October 2001.

There are three different architectures in P2P: centralized, decentralized structured and decentralized unstructured. In the centralized model like Napster [1] there is a server which stores a list of file shared by a node so a node can search the file from the server and find the whereabouts of the peer node. In the decentralized structured model there is no central server. So there is more freedom for peers to search directly or indirectly. The decentralized structured P2P models are not popularly used. The decentralized unstructured model like Kazaa [2] and Gnutella [3], where the files are placed on random nodes and they are widely used in today's internet.

In the paper, we propose an architecture, which is a combination of both centralized, and decentralized unstructured P2P systems which will be explained in section III and section IV. Section V discusses future work and concludes the paper.

II. RELATED WORKS

Research in P2P file share systems in past few years is mostly based on file look up mechanisms. P2P networks have proven a better alternative to traditional client-server systems when it comes to resources sharing. Mostly the research is related to performance, how to improve the file share network and search speed. The problem of free riding and trust based mechanics where not given any importance until past few years they where the topic for research the first free riding file share was reported in September 2000 and the trust based methods are still under research. Our work gives some solution to these problems as provides a method to remove the free riders and assign trust to users for safer download.

Different works in this regard has been done. Some of them are [4][5][6][7][8].

III. PP-FSM: PEER TO PEER FILE SHARE FOR MULTIMEDIA

The aim of PP-FSM is to provide a file share system for multimedia data on P2P network to be safer, trusted and free from free riders (resources should be given to only those users which share there resources with other users). As discussed in Section I that PP-FSM is a Hybrid based model. PP-FSM provides security to its users by assigning them trust certificate and banning the other users which do not come to its requirements or want to join the network for passing viruses and disturbing users.
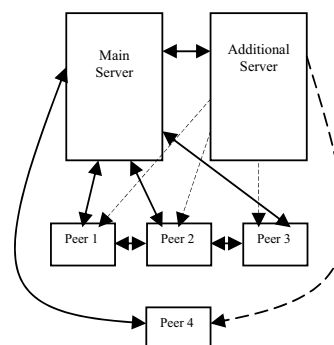

Figure I. Shows Peer Nodes

The Figure I. Shows that the nodes connecting to the network by logging to the main server listing its shared resources. The main server givens the peer information to the

Manuscript received February 15, 2005.

Arsalan Ali Shah is a student of MS at Mohammad Ali Jinnah University Islamabad (phone: +92-0300-5249770; fax: +92-51-925-7414; e-mail: sarsalan@isd.wol.net.pk).

Zafar I. Malik is a professor at Mohammad Ali Jinnah University Islamabad (e-mail: zafar@jinnah.edu.pk).

Shaukat Ali is a student of MS at Mohammad Ali Jinnah University Islamabad (phone: +92-0333-5501435; fax: +92-51-925-7414; e-mail: shukatali@ hotmail.com).

additional server to check the resources assign trust to the nodes if the resources are multimedia related and then monitors the nodes for free riding. If a node is free riding or have non multimedia related data then it will not be allowed to join the network like Peer 4. The Peer 1, 2, 3 recourses are acceptable, are not free riding they will be assign the trust certificate and will be allowed to the network for sharing file from other peer nodes connected at that time with the network.

The files shared on the PP-FSM network will be Multimedia only. Table below gives different supported formats.

Resource type	File extensions
Picture	.jpg, .bmp, .gif etc
Audio	.mp3, .wav, .ogg etc
Video	.3gp, .mpg, .mov, .rm etc
Text	.txt, .doc, .pdf, .xls etc
Archives	.zip, .rar

Table I. Multimedia Data File

IV. PP-FSM ARCHITECTURE

In this section, we will discuss architecture of the PP-FSM in detail with reference to Figure 1. The main and additional server and Peer nodes are also discussed.

A. Main Server

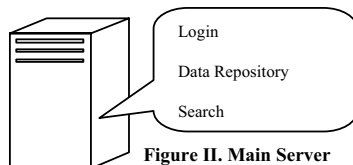The main server is the main part of the network from where all the nodes login the network.

Figure II. Main Server

The main server logins nodes on the network, take the list of recourses shared by the users, and pass it to the additional server. The additional server checks resources and monitors the nodes. The main server can also be used as a lookup server by the nodes to find the shared resources shared by other nodes connected to the network. Main server provides search feature to the nodes to use its Database repository to search on the bases off metadata. The main server has details of the nodes on the network there details and gets the feed back from the additional server.

B. Search

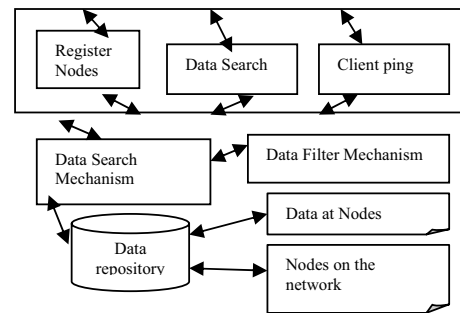The main server provides a feature of search to the nodes connected. To find the resources faster and more accurately

Figure III. Server Search

When a node wants to use the search at the server it will type the data that it wants to search the server will check the nodes connected to the network. Client ping allows the server to check for the users status. The data search can be done on the Metadata (e.g. the title, subject, author, and size) Mechanism. The data filter mechanism could include collaborative filtering techniques, for example, allowing users of the system to attach recommendations to data or the providers of data. The data repository is the database where all the details about a node are saved.

C. Additional Server

The additional server after the main server takes the responsibility of nodes on the networks. The node connected to the network does not know about the additional server it's hidden to them. It monitors them consistently and gives the feed back to the main server to take action.
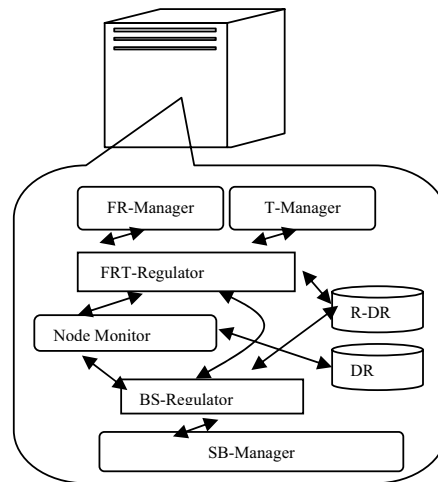

Figure IV. Additional Server

D. Node Monitor

The Node Monitor communicates with the main server giving its feed back about the nodes status. The nodes details are kept in the Data Repository. The Node Monitor gives the node information to its counterparts the FRT-Regulator and BS-Regulator that then communicate with the managers.

There are two sub modules in the Node Monitor: File Director and Feed Back module. File director checks the node for the file shared by the node as they are in requirements and as the main server need constantly feed back about the current status of the nodes connected from Feed Back module.
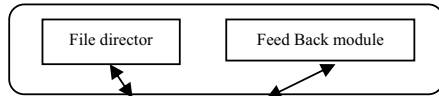

Figure V. Node Monitor

The Feed Back module takes the information of nodes from the DR and gives it to the main server.

E. Free Rider Trust Regulator (FRT-Regulator)

The FRT-Regulator which communicates with the FR and T Manager when the Node Monitor gives the node details to the FRT-Regulator it forwards the required detail to the managers and then they take the required action. Details about the nodes are saved in the (R-DR) and when required given to the Node Monitor to be forwarded to the main server.

F. Ban Security Regulator (BS-Regulator)

The BS-Regulator is like the FRT-Regulator but works with the ban and S-Manager. It takes the details from them and saves them in the R-DR and provides details to the Node monitor.

G. Free Rider Manager (FR-Manager)

The FR-Manager monitor the nodes for free riding, check their status constantly and gives it feed back to the FRT-Regulator which forwards it to the node monitor. The FR-Manager has two modules: Monitor and the FR-Assigner. The FR-Assigner communicates with the monitor when a node logins. The monitors is scheduled checks nodes status on time bases gives feed back to the FR-Assigner.
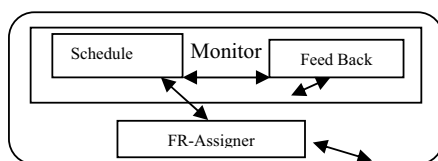

Figure VI. FR-Manager

The FR-Assigner takes details from the feed back module and if the peer node is a free rider it is banes them for some time.

H. Security Ban Manager (SB-Manager))

The SB-Manager checks the node for viruses and bans the nodes from coming on the network if they are found doing something illegal.
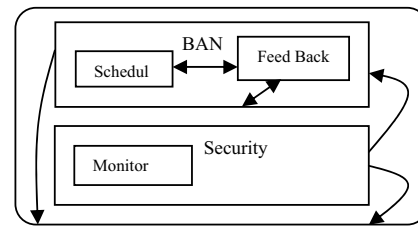

Figure VII. SB-Manager

The SB-Manager plays an important role it gives the details to the SB-Regulator about the nodes ban and for how long they have been banned and why. The ban will be on a node which is found to be free riding having virus files being downloaded by other users. The security works as it monitors the nodes, scans the files which are Archive file if they are not properly compressed up to level 1 or not. The security also checks the file for piggyback files, e.g., the files that have "abc.jpp.exe", etc. Files on the network and the new users joining the network and reports back to the BS-Regulator.

I. Trust Manager (T-Manager)

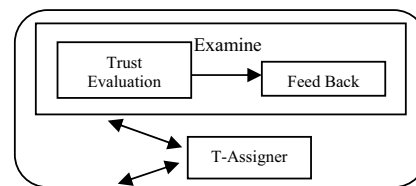The T-Manager is another important part of the system assigns trust certificate to the users.

Figure VIII. T-Manager

The T-Manager works as the node detail is given to the T-Assigner which gives the details to the Trust Evaluation which assigns the certificate and if a node loses its trust for some reason then the process is repeated all over again.

J. Data Repository (DR) and Regulator - Data Repository (R-DR)

The R-DR saves the details of nodes for ban, security, trust, and free riding. If a node is already login, the process is not repeated again the R-DR should be there for the details to be given to the Node monitor about the update which takes places after 15mins or so.

The DR is the main repository where the details about the nodes are saved what action should be taken, details about the past actions, new nodes joining and carries the details of data which each node within the system is making publicly available.

K. Peer Nodes

In this section, we will discuss main parts of the peer nodes on the network like the main and additional server the peer nodes holds the data which they have shared and list their shared resources to the server.
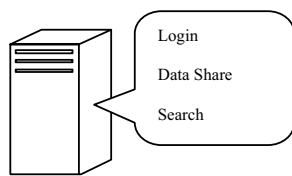
Figure IX. Peer

The nodes login the server to gain access to the network, list down shared resources which it wants to share then goes through the process of PP-FSM. The servers for security and free riding constantly monitoring the data shared by the nodes. The node when joins the network list the resources if the resources are changed at any time later the Node Monitor monitors the update and checks the files for security. The PP-FSM is related to multimedia files, which will be shared as they are larger and carry a lot of data size. The nodes can find the shared resources from other nodes as well from the server. The server keeps the list to shared resources by the node in its data repository and keeps it updated for future use.

L. Search

The server and nodes provide the search feature but the server search is only there for reference. Nodes can not download the data using the server only node to node is allowed in the network the nodes can see the list of resources shared by the nodes from the server and download it from the node.
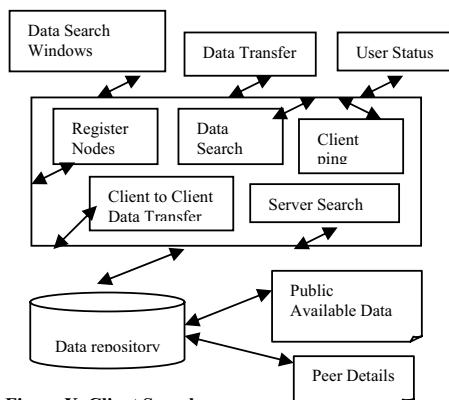

Figure X. Client Search

The search works when nodes are registered to the server and connected the node can search the references from the server as well from the other nodes connected to the network. Client to client data transfer needs to support the exchange of data with other clients. Publicly Available Data this represents the data that the node is making available to the system. Peer Details keeps the data details on the nodes, as well the resources (bandwidth, etc).

V.CONCLUSION and FUTURE WORK

In this paper, we have proposed a new P2P architecture for multimedia files. The PP-FSM is a hybrid system two servers

and nodes. The servers work consistently with each other and monitor the nodes for the shared resources and free riding. The servers work as a new node joins the network the main server gives the details to the additional server checks the node for shared files and forwards to the SB-Manager where it is checks for viruses then to the FRT-Regulator for checking of free riding and trust and allowed them to the network and details are kept in the DR of the server. If a node is already on the network and the shared resources are stopped the additional server checks the node data updates the DR and R-DR and forward to the SB-Manager which will be BAN the node. The system may have some problems but provides features like search, free riding and trust to its users for security.

Currently, we are developing a prototype tool based on PP-FSM architecture. Results of this tool will be then compared with existing architectures.

REFERENCES

[1] Napster, http://www.napster.com
[2] KaZA, http://www.kazaa.com
[3] Gnutella, http://gnutella.wego.com
[4] Morpheus website. http://www.morpheus-os.com
[5] Li X., L. Liu, PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities. IEEE Transactions on Knowledge and Data Engineering , vol. 16, no. 7, July 2004
[6] L. Ramaswamy and L. Liu. Free riding: A new challenge to peer-to-peer file sharing systems. Technical report, College of Computing, Georgia Institute of Technology, Atlanta, 2002.
[7] M. Karakaya, I. Korpeoglu, and ¨O. Ulusoy. A distributed and measurement-based framework against free riding in peer-to-peer networks. Technical Report BU-CE-0405, Department of Computer Engineering, Bilkent University, May 2004.
[8] M. Andreolini R. Lancellotti P. S. Yu. Analysis of peer-to-peer systems: workload characterization and effects on traffic cacheability. In Proceedings of the IEEE Computer Society's 12th Annual International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunications Systems (MASCOTS'04), 2004.