Collaborative Peer-to-Peer Service for Information Sharing Using JXTA

Hao Shi[1], Yanchun Zhang[1], Jingyuan Zhang[1], Elizabeth Beal[2], Nick Moustakas[2]
School of Computer Science and Mathematics[1]
Victoria University, Australia
{hao.shi, yanchun.zhang}@vu.edu.au, jing.zhang7@students.vu.edu.au
Communications Law Centre[2]
Melbourne, Australia
{ebeal, nmoustakas}@comslaw.org.au

Abstract

Peer-to-Peer (P2P) file sharing networks attract much attention from legal and research communities. The success and popularity of P2P networks provides a new paradigm for sharing and distributing information. However, the widespread illegal distribution of the copyright protected works and anonymous malicious attacks to the network raise serious concerns for the future of P2P applications. Legal and research professionals face a challenge to collaboratively develop a P2P application that reduces these concerns. Our research aims to develop a P2P collaborative research network, named vuCRN, for legal academics and researchers to facilitate document sharing. In this paper, we present our vuCRN prototype based on JXTA technology. JXTA provides services to let peers find each other in the group, and exchange messages across firewalls and NATs (Network Address Translators). vuCRN allows, peers to freely download shared files but their upload permission is controlled by decentralized user authentication, using local LDAP (Lightweight Directory Access Protocol) servers. This ensures that peers in vuCRN network obtain only reliable information and protects the quality of resources. This prototype is fully tested in LAN (Local Area Network), Internet and inter-university networks. The testing results, conclusions and future work are also presented in this paper.

1. Introduction

P2P network have become one of most popular Internet applications [1, 2]. P2P networks provide many benefits over standard client-server approaches for file sharing [3]. P2P architecture allows for rapid expansion of networks and rapid distribution of each resource within the network [4]. The ultimate goal of this research is to develop a collaborative research network that supports research across multiple disciplines, industries and sectors by providing a reliable mechanism for an open exchange of information. The preliminary aim of the research is to develop a P2P network prototype that enables effective control over who can upload content using the existing user authentication. Further the research aims to develop a prototype that issues a range of "machine or network readable" licenses to attach to files that are uploaded to the network whilst simultaneously facilitating free public access to material on the network. This research involves collaboration between legal and research professionals and aims to collaboratively create a research network for sharing legal documents. The research is both technology and application driven. From an application point of view, the application will include both copyright licensing information and digital rights management ("DRM") information over the P2P network. Existing P2P networks allow peers to upload and download files from the P2P network, however, current P2P network protocols don't address licensing or document management issues and quite often the P2P network is 'polluted' with inauthentic files. The success rate for finding useful documents/materials is very slim on existing p2p networks and current usage of P2P network continues to be primarily for music, films and software file sharing rather than research materials [5, 6, 7]. From a technology point of view, this research will use existing open source technologies to create the collaborative research network and eventually the source codes of this application will be made available online to public.

In this paper, we present our *vuCRN* prototype based on JXTA technology. P2P technologies and file sharing are reviewed in the next section. Section 3 briefly describes *vuCRN* architecture including JXTA, myJXTA and LDAP. Design and implementation of the prototype including its PeerGroup management, file sharing and the system testing results are described in Section 4

Proceedings of the First International Multi-Symposiums on Computer and Computational Sciences (IMSCCS'06)
0-7695-2581-4/06 $20.00 © 2006 IEEE

respectively. Conclusions and future work are presented in the last section.

2. P2P technologies

2.1. P2P architectures

There are various popular P2P network architectures such as Napster launched in 1999, Gnutella launched in 2000, FastTrack launched in 2001 and JXTA launched in 2001 [8, 9, 10, 11]. Napster is an online music service which was originally a file sharing service created by Shawn Fanning in 1999 [12]. The architecture of Napster pioneered the concept of peer-to-peer file sharing with each user's computer connecting to Napster's central server. The Napster server held a complete index of files available on each client computer that was connected to the Network. The Napster server however did not store any files. Users of the Napster network were able to share files stored on users or "client" computers after locating a file sought through searching the Napster index on its central server. The disadvantage with this model is that once the Napster central server is shut down, the complete network disappears because users are unable to search for files.

Gnutella was developed by Justin Frankel and Tom Pepper of Nullsoft in early 2000 [13]. It is a peer-to-peer network similar to Napster, but without a centralized server. If the client of Gnutella can satisfy the sever requirements, it can be both a server and a client. The main advantage of Gnutella over Napster is the fact that it is decentralized; which means that there is no single server that can be shut down. As long as a user can connect to at least one other machine, Gnutella will always work. Based on the decentralized concepts brought forth by Gnutella, FastTrack subsequently emerged as the next king of file sharing. The FastTrack protocol was developed by an Estonian programmer Jaan Tallinn and his Scandinavian partners Niklas Zennström and Jaanus Friis, the same team that created Skype [14]. It was launched in March 2001 by their Dutch company Consumer Empowerment [14]. The FastTrack protocol operates, under the flags of KaZaA, Grokster and iMesh and is often referred to as a hybrid network because it uses decentralized supernodes to act as temporary indexing servers [15].

The strength of P2P technology is its decentralization which allows for it to be completely robust not relying on centralized servers or particular users. The potential for P2P technology is great but has yet to be maximized. P2P technology has been particularly popular with sharing music files, software, and video files. Theoretically, peers at any computers attached to the Internet can directly connect to each other and exchange messages between them using the TCP/IP protocol suite. However, the wide existence of firewalls and NATs currently in place on the Internet often makes direct peer connections very difficult or even impossible via TCP/IP [16]. Pure Napster, and Gnutella like approaches are not suitable for an open exchange of research information because many educational institutions block such networks from getting into their firewalls due to security concerns.

JXTA framework provides a set of protocols and a series of services that let peers to find each other, form groups and directly exchange messages [11][16, 17]. The JXTA is a decentralized (pure) P2P architecture and the JXTA network is a dynamically created ad hoc network without a central control or server. These features of JXTA and its capability to interact with peers behind firewalls and NATs, JXTA was chosen as the platform from which to design and implement our P2P network prototype.

2.2 P2P File Sharing the Pros and Cons

P2P networks don't require users to authenticate before logging on to the network although some networks may require registration for identification. There is no access control on file sharing networks except the distinction between shared and unshared files. Shared files are available to everyone; unshared files are available to none [18]. Peer-to-peer file sharing networks have many benefits over standard client-server approaches to data distribution, including increased robustness, scalability, and diversity of available data [18]. However, the open and anonymous nature of these networks results in a complete lack of accountability for any content uploaded onto the network, opening the door to abuses of these networks by malicious peers [18].

Attacks by anonymous malicious peers have been observed on popular peer-to-peer networks such as Gnutella. For example, malicious users have used these networks to introduce viruses such as the VBS.Gnutella worm, which spreads by making a copy of itself in a peer's Gnutella program directory and then modifying the Gnutella.ini file to allow sharing of .vbs files [18]. Far more common have been inauthentic file attacks, wherein malicious peers respond to virtually any query providing "decoy files" that are tampered-with or do not work. As a result, decentralized P2P networks attempt to build reputation systems to accurately track and measure the peers' activities on the network [18, 19]. The disadvantage is that the reputation measurements create overhead expenses and anonymous malicious peers will always exist. Certainly the situation in the structured environment such as the university networks is different. User authentication, access control, and logging are mandatory. In order for a file sharing network to thrive in an academic environment, security is the highest priority.

The proposed P2P research network will require users to authenticate upon upload of files in order to ensure the quality of resources on the network and help prevent inauthentic files.

3. *vuCRN* architecture

3.1. JXTA P2P framework

JXTA (Juxtapose) is an Open Source de-centralized peer-to-peer platform created by Sun Microsystems in 2001. It allows any device connected to a network to exchange messages and collaborate in spite of the network topology. JXTA is the most mature P2P framework currently available [20] and becomes a generic platform for implementing any kind of P2P applications [21].

JXTA is an open network computing platform designed for P2P computing. In essence, JXTA provides a set of XML based protocols to cover typical P2P functionality. Its goal is to develop basic building blocks and services to enable innovative applications for peer groups [22]. JXTA software architecture is divided into three layers, as shown in Figure 1 [16].

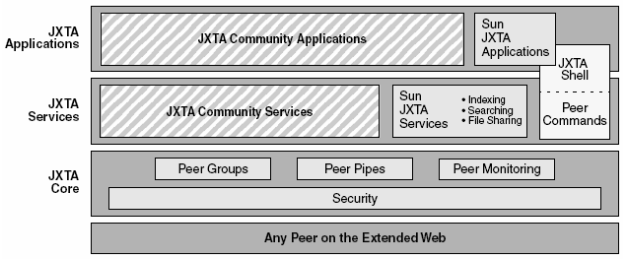

Figure 1. JXTA architecture [16]

JXTA peers create a virtual network where any one peer can interact with other peers and resources directly even when some of the peers and resources are behind firewalls and NATs (Network Address Translators) or are on different network transports [16]. Peers use protocols defined by JXTA to discover each other, advertise and discover network resources, and communication and route message. The peer can be discovered by Peer Discovery Protocol (PDP). PDP is default discovery protocol for all users in defined peer groups and default net peer groups. Each group has at least one rendezvous peer, all peers of that group connect to the rendezvous peer. All the groups connect by the rendezvous peer. If a peer joins a group and doesn't find a rendezvous peer, it will become rendezvous. All peers will connect to several groups by default, in case one of the group's rendezvous peer is offline the network still exists [16]. After peers connect to the network, the shared file can be searched by a combination of IP multicast to the local subnet and the use of rendezvous peer. After identifying matching responses the connection to a download file can be set. Client can search the peer by specify the user ID, and chat privately. All types of files can be shared on the JXTA network.

3.2. MyJXTA

MyJXTA is a JXTA Technology based collaboration application, designed from the ground up to be easy to use, modify, extend and deploy [23]. It is an exemplary JXTA application that strives to showcase JXTA best practices for all core lib/apis via deployments of massive scale and provide a framework which people can learn from and build upon. Features include group chat, secure 1 to 1 chat, anonymous and credentialed group create / find/ join/ leave, share / search/ publish/ view/ store, group search, message listener/ filter/ directive interfaces [24].

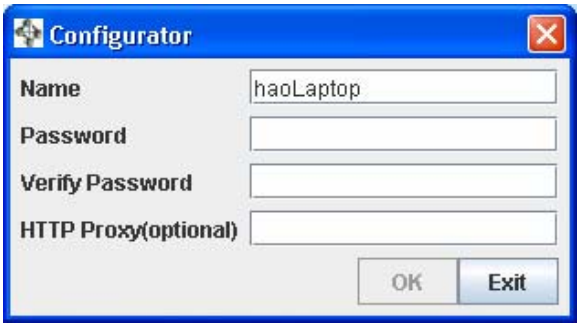

Figure 2. MyJXTA Registration

When running MyJXTA for the first time a peer will be prompted for registration information that includes the peer's name and a certificate pass phrase as shown in Figure 2, the later of which is used to initiate secure communications via JXTA membership authentication. The JXTA network is shown in Figure 3 and its Graph Galore is illustrated in Figure 4. After successful registration with the system, the peer is in a default JXTA group called "NetPeerGroup", which is a big umbrella of all JXTA peers.

3.3. *vuCRN* File Sharing

The challenge for peer authentication in a decentralized P2P network is to identify peers and to grant upload permission in another administrative domain, without assuming any kind of pre-existing administrative relationship. The traditional approach to user authentication across administrative domains is for users to prove their identities through a chain of

certificates. However, certificates cannot be validated as there is no central server in a decentralized P2P network. Our approach is to use local authentication servers to establish identities for users based just on local information. When peers attempt to upload their files, the local authentication will be activated and permission will be granted after successful authentication. The above procedures are detailed in a sequence diagram in Figure 5.

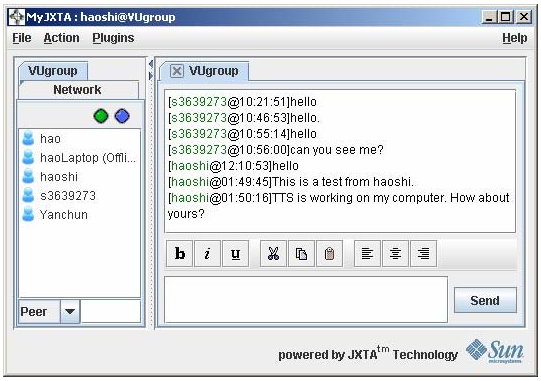

Figure 3. JTXTA network

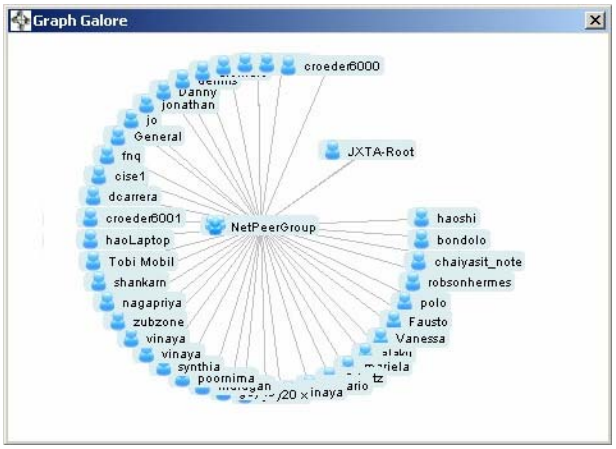

Figure 4. NetPeerGroup

Although users may have multiple accounts, LDAP (Lightweight Directory Access Protocol) is a central server in an organization and it combines several systems that normally have to be maintained separately by NT authentication or UNIX authentication [25]. LDAP allows information such as userID and passwords for an entire site to be stored on a central location and provide a standard method for user authentication especially at educational institutions. A typical LDAP contains Host, Base DNS and User DN as shown in Figure 6.

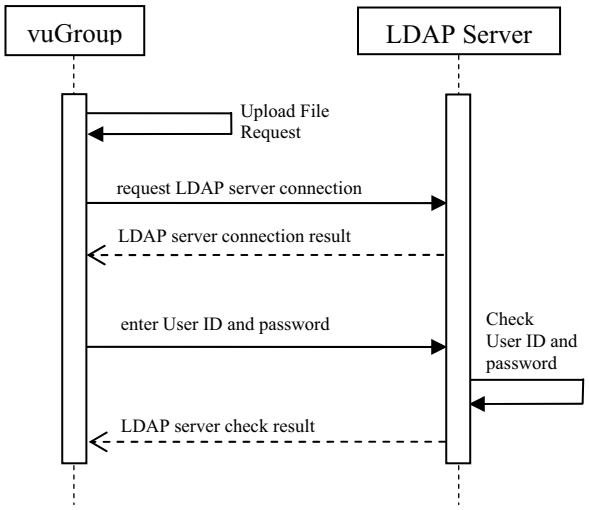

Figure 5. A sequence diagram of LDAP authentication

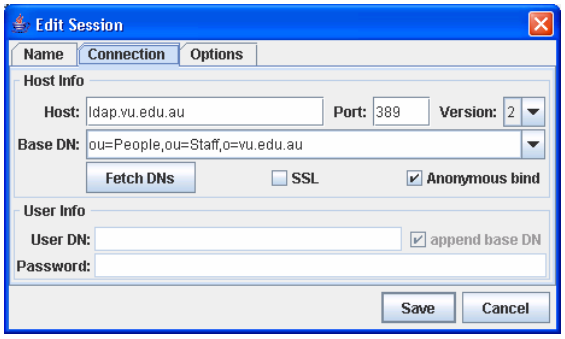

Figure 6a. Connection tab of LDAP browser

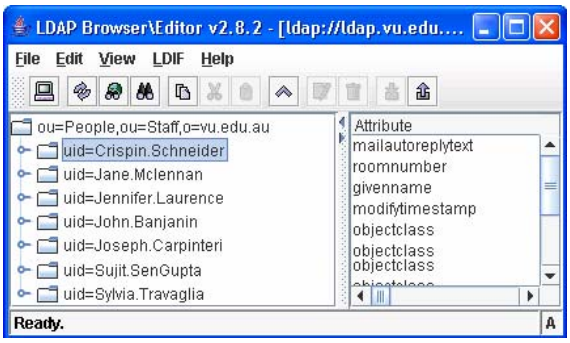

Figure 6b. LDAP structure

4. Prototype implementation

Our implementation is based on JXTA protocol using myJXTA user interface. We have made two significant improvements to the existing MyJXTA application in order to build a collaborative research network prototype: peer group establishment and decentralized LDAP authentication.

4.1 Peer Group establishment

Peers in *vuCRN* have been organized into a peergroup called 'vuGroup' that has a unique peergroup ID for isolation from other peergroups in the JXTA network and to enable peers in the group to locate the 'vuGroup'. An example of a peergroup can be set as shown in Figure 7. The underlying JXTA core peergroup services provides the basic functionality to support the 'vuGroup' existence (publishing and discovering resources and exchanging messages) with their associated protocols (discovery, resolve, pipe, peer info, and rendezvous).

After a peer successfully logs into the system the GUI will appear and all the peers are in a default JXTA group called "NetPeerGroup" and also automatically sign in the 'vuGroup' as shown in Figure 8.

```
- <myjxta>
    <application name="MyJXTA" version="2.3.6"
      build="2005.12.16:00.37.09 +0000" />
    <proxy http="" />
  - <network>
      <group id="urn:jxta:uuid-
        19891014140020000815180024441026O2"
        name="VUgroup" password="" description=""
        autoRendezVousPeriod="120000" />
    </network>
    <resources
      strings="net.jxta.myjxta.resources.text.strings"
      theme="/net/jxta/myjxta/resources/themes/crystal-
      gaim/theme.txt"
      chatStyle="/net/jxta/myjxta/resources/html/chat.css" />
    <chainsaw host="localhost" port="4445"
      reconnect="10000" locationInfo="true" />
  </myjxta>
```

Figure 7. An example of peergroup setting

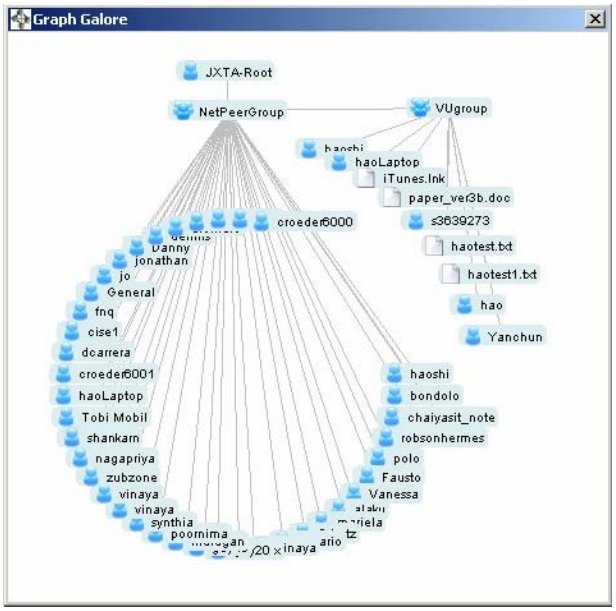

Figure 8. Peers in 'vuGroup' peergroup

4.2 Decentralized LDAP authentication

Although MyJXTA comes with login procedure, it is purely used to locate the peer on the network. Every user who installs JXTA can create a user account like other P2P networks. As mentioned in Section 3.3, we propose to use local LDAP servers for authenticating decentralized users. The actual action is implemented at the Share menu as shown in Figure 9 where users upload their files on the network.

There are three steps in LDAP operation:

- local LDAP server identification
- LDAP connection
- User authentication by user ID and password

Novell Java package is used to develop the LDAP operations methods. The program first sets the LDAP server's name and connection string as shown in Figure 10. Then it tests the LDAP server connection. If the LDAP is present, the connection will be successful, otherwise it will fail. Once the users choose Share File action, it will trigger the LDAP to authenticate the user by user ID and password. If it is not successful, the authentication window will be popped up to ask the user to re-enter the user ID and password. If it is successful, users can choose the files from the local disk and share them on the JXTA network. Without the successful authentication by the local LDAP server, the users won't be able to upload files rather they can only download files from the network. This guarantees that all peers sharing a JXTA network are authenticated by a local LDAP server.

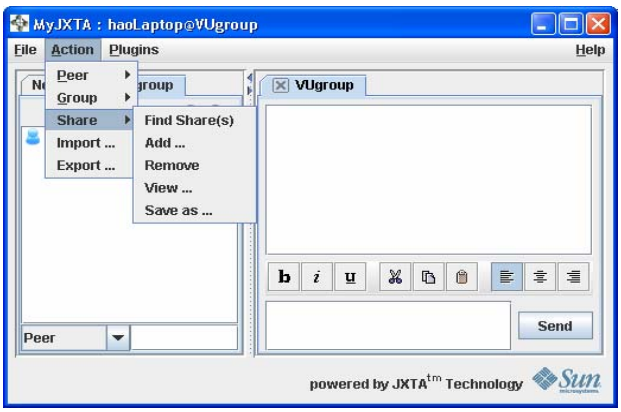

Figure 9. Upload Control using LDAP

4.3 System Testing

The system has been intensively tested during its development and implementation. The testing has been conducted in LAN (local area network), Intranet, Internet, and inter-university networks.

```
import com.novell.ldap.LDAPAttribute;
public class LDAPOperations {
    private final int LDAP_PORT = LDAPConnection.DEFAULT_PORT;
    private final int SEARCH_SCOPE = LDAPConnection.SCOPE_SUB;
    private int LDAP_VERSION = LDAPConnection.LDAP_V3;
    /**  setting for LDAP **/
    private final String searchBase = "o=vu.edu.au";
    private final String HOST = "ldap.vu.edu.au";
    private final String staffLogin = ";ou=People;ou=Staff;o=vu.edu.au";
    private final String studentLogin = ";ou=Current;ou=Students;o=vu.edu.au";
    /**  Description of the Field **/
    public char USER_TYPE;
...
    /** Connect to LDAP server anonymously **/
    public int connectToServer() {
        lConnect = new LDAPConnection();
        try {
            lConnect.connect(HOST, LDAP_PORT);
            }
        catch (LDAPException e) {
            return -1;
        }
        return 1;
    }
...
}
```

Figure 10. LDAP operations

There are two major focuses:

- 'vuGroup' management
- user authentication by LDAP

4.3.1 'vuGroup' testing

NATs. If no other peer exists in the group, it will act as a rendezvous. Others using original MyJXTA cannot have access to 'vuGroup' but stay in MyJXTA group as JXTA promises that every private peergroup is a security [26,27]. The tests show that peers in the 'vuGroup' can send each other messages correctly and 'vuGroup' is functioning like a collaborative group.

4.3.2 Upload testing

At Victoria University, the testing is first conducted at research labs, and later moved to individual staff offices, then private homes via Internet. User authentication is activated every time when peers try to upload the file to the 'vuGroup' as shown in Figure 10. Users have been successfully authenticated at LAN and Intranet by its local LDAP as shown in Figure 11a but failed at private homes as LDAP resides inside the University firewall and no connection can be established outside the firewall as shown in Figure 11b. In this case, the Internet users need to install VPN (Virtual Private Network) to be able to upload their files.

When the tests are conducted at other universities, the major task is to configure the LDAP setting because they vary from university to university. For example, LDAP at VU is ldap.vu.edu.au and at Monash University is directory.monash.edu.au. The tests are successfully conducted at different universities with their central LDAP servers. This guarantees that upload control for the purposely built research network can be implemented through the educational system. Currently a LDAP-based project called 'Federations and Secure Access' [28] is being carried out in order to solve the problems of access and identity management in distributed and secure environments. Eventfully it will expand the current approach to a larger scale.

(a) Success

(b) Failure

Figure 11. LDAP connection

5. Conclusions and future work

The primary goal of the proposed Network is to provide a P2P network that has an unlimited potential for collaboration between academics and researchers. File sharing is only the beginning for the proposed P2P Network. Lionshare [29] has pioneered in this area but it is a centralized P2P network based on Limewire [30]. The application of P2P file sharing has the potential to evolve into a system that serves as a convergence for a variety of technologies and applications. The success of this developed network prototype for file sharing will contribute to the advancement of knowledge and the development of P2P systems in non-traditional applications. Its success shows great promise for further development of a collaborative research network for academics and researchers to facilitate legal document sharing. It would greatly promote cross boundary collaborations, and become an important source for creative works. It would pave a way to overcome legal barriers for P2P network to share resources. It will eventually help to expand such collaborative research network to facilitate collaborative research across various disciplines.

Acknowledgements

This research (ID: SR0567506) was supported by ARC e-Research grant from Australian Research Council. The authors would also like to acknowledge support from Communications Law Centre and School of Computer Science and Mathematics at Victoria University.

References

[1] Androutsellis-Theotokis, S. and Spinellis, D. (2004) "A Survey of Peer-to-Peer Content Distribution Technologies", ACM Computing Surveys (CSUR), Vol. 36, No. 4, December 2004, pp. 335 - 371.

[2] Gibbs, M. (2003) "Peer-to-Peer: Past, Present, and Future", http://www.hill.com/archive/pub/papers/2003/03/paper.pdf.

[3] Philip E. Agre, (2003) "P2P and the promise of internet equality", Communications of the ACM, Vol. 46, No. 2, February 2003, pp. 39 – 42.

[4] Clarke, R. "Towards a P2P Research Agenda", (2005), http://www.anu.edu.au/people/Roger.Clarke/ EC/P2PRes.html.

[5] Riehl, D. A. (2001) "Peer-To-Peer Distribution Systems: Will Napster, Gnutella, and Freenet Create a Copyright Nirvana or Gehenna?", William Mitchell Law Review, Vol. 27, pp. 1761-1781.

[6] Colletti, D. J. (2003) "Technology Under Siege: Peer-To-Peer Technology is The Victim of the Entertainment Industry's Misguided Attack", George Washington Law Review, No. 71, pp. 255-265.

[7] Ennis, D., Anchan D., and Pegah, M. (2004) "The Front Line Battle Against P2P", SIGUCCS'04, October 10-13, 2004, Baltimore, Maryland, USA, pp. 101-106.

[8] Philip E. Agre, "P2P and the promise of internet equality", Communications of the ACM, Vol.46, No. 2, February 2003, pp.39-42.

[9] Riehl, D.A., "Peer-To-Peer Distribution Systems: Will Napster, Gnutella, and Freenet Create a Copyright Nirvana or Gehenna?" *William Mitchell Law Review*, Vol.27, pp.1761-1781.

[10] Gibbs.M., "Peer-to-Peer: Past, Present, and Future", http://www.hill.com/archieve/pub/papers/2003/ 03/paper.pdf.

[11] JXTA v2.3.x: JavaTM Programmer's Guide, Sun Microsystems Apr 7, 2005 pp.11-27.

[12] Napster, http://en.wikipedia.org/wiki/Napster

[13] Gnutella, http://en.wikipedia.org/wiki/ Gnutella

[14] FastTrack http://en.wikipedia.org/wiki/Fast Track

[15] Sen, S. and Wang, J, "Analyzing Peer-to-Peer Traffic Across Large Networks", IEEE/ACM Transactions on Networking, vol. 12, No. 2, April 2004, pp. 219-232.

[16] Li Gong. "Project JXTA: A technology overview". Technical report, SUN Microsystems, April 2001. http://www.jxta.org/project/www/ docs/ TechOverview.pdf.

[17] J. Ma, M. Shizuka, J. Lee and R. Huang, "A JXTA-based Synchronous Collaborative System with Decentralized Topology", May 2003, http://www.jxta.org/research/hosei_univ.pdf.

[18] S. D. Kamvar, M. T. Schlosser, and H. GarciaMolina, "The EigenTrust Algorithm for Reputation Management in P2P Networks", Proc. of the 12th Int. Conf. on World Wide Web, WWW2003, Budapest, Hungary, May 20–24, 2003, pp. 640 - 651.

[19] Minaxi Gupta, Paul Judge, Mostafa Ammar, "A Reputation System for Peer-to-Peer Networks", NOSSDAV'03, Proc. of the 13th Int. workshop on Network and operating systems support for digital audio and video, June 1–3, 2003, Monterey, California, USA, pp. 144 – 152.

[20] JXTA, http://en.wikipedia.org/wiki/JXTA

[21] W. Nejdl, B. Wolf, C. Qu, S. Decker, M. Sintek, A. Naeve, M. Nilsson, M. Palmér, T. Risch, "EDUTELLA: a P2P networking infrastructure based on RDF", Proc. of the 11th Int. Conf. on World Wide Web, WWW2002, May 7–11, 2002, Honolulu, Hawaii, pp. 604 – 615.

[22] JXTA, http://www.jxta.org/.

[23] MyJXTA, http://myjxta2.jxta.org/

[24] MyXTA, http://en.wikipedia.org/wiki/ MyJXTA.

[25] Barman, A. "LDAP application development using J2EE and .NET", India Annual Conference, 2004, Proceedings of the IEEE INDICON 2004, 20-22 Dec. 2004, pp.494 – 497.

[26] Loesing, K.; Wirtz, G., "An implementation of reliable group communication based on the peer-to-peer network JXTA", Computer Systems and Applications, The 3rd ACS/IEEE International Conference on 2005 pp.82-89.

[27] Z. Li; Y. Dong; L. Zhuang; J. Huang, "Implementation of secure peer group in peer-to-peer network", Communication Technology Proceedings, ICCT 2003. International Conference on Volume 1, 9-11 April 2003, pp.192 – 195.

[28] J. Dalziel, "Federations and Secure Access - Beyond DRM",http://www.aarnet.edu.au/engineering/middleware/archive/middle/2004/forum/Dalziel.pps, AARNet Middleware Camp 2004.

[29] LionShare, http://lionshare.its.psu.edu/main/

[30] LimeWire, http://www.limewire.org