ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I6M7-112012

VOLUME 2 ISSUE 6 November 2012

A PRAGMATIC ANALYSIS OF PEER TO PEER NETWORKS AND PROTOCOLS FOR SECURITY AND CONFIDENTIALITY

Anil Saroliya[1], Upendra Mishra[2], Ajay Rana[3]

[1]Department of Computer Science, Amity University Rajasthan, Jaipur, India;

[2]Department of Mathematics, Amity University Rajasthan, Jaipur, India;

[3]Department of Computer Science, Amity University Utter Pradesh, Noida, India;

ABSTRACT

The internet as we ought to understand it is a dramatized environment that links together various information, networks and communication channels. However, the bitter truth lies in the fact that the Internet has largely grown into a drone that lacks essential centralized control. Putting into simpler terms, with the day by day growth of the Internet, it is simply beginning to lack any hierarchical control. With this growth, comes the need of large scale data distribution, content sharing and multicasting applications. In other words, the need of the hour lays in extensive use of Peer-to-Peer (P2P) networks. The P2P networks are loaded with the abilities to provide many handy features such as selection of most accurately reachable peers, powerful search mechanisms or location of data together with hierarchical name stay. The P2P networks have the special ability to organize and handle self-framed routing architecture that also helps in measuring massive scalability and hence provides a robust and efficient load balance of the world wide network or simply the Internet. Despite the numerous merits of P2P Networks over the near obsolete client- server mechanisms, there have also been some shortcomings in the same. Most prominent of these shortcomings include various vulnerabilities within the P2P applications. This arouses the need of skeptical sense and awareness among both the users and Network Administrators pertaining to the illegitimate and malicious content found on the P2P Network. Certain security measures are needed to be monitored by the Network Administrators to prevent

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I6M7-112012

VOLUME 2 ISSUE 6 November 2012

breaches and leaks of crucial information in case of corporate networks. The measure can be one such that minimizes a set of firewalls to allow the traffic and at the same time maintain the critical compilation with corporate security and confidentiality. Home users must also ensure security through the use of up to date firewalls in order to minimize malicious threats to their machines. This paper deals with the comparison and opinion of P2P Networks in terms of both security and confidentiality.

KEYWORDS - Network Confidentiality, Network Integrity, Network Vulnerability, Peer To Peer Networks, Security Protocols

1. INTRODUCTION

In traditional internet and intranet networks, the applications are client-server based, many of them communicating with a common shared server for application services. Some examples of such applications include e-mail servers, web servers and file servers. However these servers have two big fundamental problems - scalability and resilience. Right now, millions of users are able to use the same internet server at the same time. Hosting a server for millions of users and staying online continuously is hard, so an alternative to the classic client-server architecture is the P2P architecture model.

In the Peer-to-Peer network architecture, each client is also a server and the coordination and discovery issues of these decentralized networks are central. P2P networks are a solid alternative network model to the classic and traditional client-server architecture. P2P networks arrange each machine, referred to as a peer, to function and play the role of a client and a server with full server functionalities at the same time. One peer can initiate requests to the other peers on the network and respond to incoming requests from other peers on the network at the same time. In traditional client-server models, a client can only send request to a server and then wait for the server's response. The server performance in a client-server model deteriorates as the number of clients requesting services increases. In

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I6M7-112012

VOLUME 2 ISSUE 6 November 2012

P2P networks, as the number of peers increases so does the performance. The peers can organize themselves into ad-hoc groups, communicating, collaborating and sharing the bandwidth facilitating the completion of each other's tasks like file sharing, communication, etc. Each peer has the ability to upload and download at the same time, making it possible for new peers to join the network and old ones to leave without affecting the network performance. The re-organization dynamic of peer-to-peer member groups is always transparent to end-users.

Peer-to-Peer networks also have a greater fault-tolerance compared to the classic client-server networks. When a peer is disconnected from the network, the application will continue by using other peers. One example of such a network is the Bit Torrent network. Any clients that are downloading one file, act as an uploading server for the same file. When a client finds one unresponsive peer, it searches for other peers, picks up parts of the file where the old peer was, and continues the download process. So compared to classical client-server networks, Peer-to-Peer networks are more fault-tolerant and more self-conserving.

2. PEER-TO-PEER NETWORKS

Peer-to-Peer networks are divided into 2 classes, Structured and Unstructured. The structured P2P is an overlay network with a tightly controlled topology, and content placed at specified locations rather than at random peers, to make queries more efficient. The structured P2P networks use the Distributed Hash Table (DHT) as a substrate, in which data object location information is placed deterministically, at the peers with identifiers corresponding to the data object's unique key. Distributed Hash Tables are structured as compared to flooding protocols like Gnutella. This means that participating nodes cannot make random links in the overlay network. Each DHT protocol defines how nodes should form connections in the overlay network, how those nodes should deal with new nodes joining, and how they should deal with nodes leaving and failing. More importantly, the protocols also define how lookup messages should be forwarded through the system. Three popular DHTs that have received a great deal of research attention include CAN, Chord, and

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I6M7-112012

VOLUME 2 ISSUE 6 November 2012

Pastry. Although DHTs can vary greatly from one another, there are a few things that almost all of them share in common.

In the unstructured P2P networks, the peers are organized on a graph in a flat or hierarchical manner and use flooding or random walks or even expanding TTL search times on the graph to query content stored by the overlay peers. Each peer supports complex queries and evaluates queries locally on its own content. Unstructured networks are more robust and support general search facilities, both of these qualities being important to P2P file-sharing and communications. Thus, the unstructured P2P system is a better approach than turning to DHT-based systems for mass-market file-sharing applications.

2.1 CONTENT ADDRESSABLE NETWORK (CAN)

The Content Addressable Network[1] known as CAN is a distributed decentralized P2P infrastructure that provides hash-table functionality on an Internet-like scale. CAN is designed to be a scalable, fault-tolerant, and self-organizing system. The architectural design is a virtual multi-dimensional Cartesian coordinate space on a multi-torus. This D-dimensional coordinate space is completely logical. The entire coordinate space is dynamically partitioned among all the peers in the system such that every peer possesses its individual, distinct zone within the overall space. A CAN peer maintains a routing table that holds the IP address and virtual coordinate zone of each of its neighbors in the coordinate space . A CAN message includes the destination coordinates and using the neighbor coordinates, a peer routes a message toward its destination using a simple greedy forwarding to the neighbor peer that is closest to the destination coordinates. The lookup protocol retrieves an entry corresponding to key K, and any peer can apply the same deterministic hash function to map K onto point P and then retrieve the corresponding value V from the point P. If the requesting peer or its immediate neighbors do not own the point P, the request must be routed through the CAN infrastructure until it reaches the peer where P lays. A peer maintains the IP addresses of those peers that hold coordinate zones adjoining

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I6M7-112012

VOLUME 2 ISSUE 6 November 2012

its zone. This set of immediate neighbors in the coordinate space serves as a coordinate routing table that enables efficient routing between points in this space.

2.2 CHORD

Chord[2] uses consistent hashing to assign keys to its peers. Consistent hashing is designed to let peers enter and leave the network with minimal interruption. This decentralized scheme tends to balance the load on the system, since each peer receives roughly the same number of keys, and there is little movement of keys when peers join and leave the system. In a steady state, for a total of N peers in the system, each peer maintains routing state information for about O other peers. This may be efficient but performance degrades gracefully when that information is out-of-date. The consistent hash functions assign peers and data keys an m-bit identifier using SHA-1 as the base hash function. A peer's identifier is chosen by hashing the peer's IP address, while a key identifier is produced by hashing the data key.

The length of the identifier must be large enough to make the probability of keys hashing to the same identifier negligible. Identifiers are ordered on an identifier circle module 2m. Key k is assigned to the first peer who's identifier is equal to or follows k in the identifier space. This peer is called the successor peer of key k, denoted by successor (k). If identifiers are represented as a circle of numbers from 0 to 2^{m-1}, then successor (k) is the first peer clockwise from k. The identifier circle is called the Chord ring. To maintain consistent hashing mapping when a peer n joins the network, certain keys previously assigned to n's successor now need to be reassigned to n. When peer n leaves the Chord system, all of its assigned keys are reassigned to n's successor. Hence, peers join and leave the system with the performance of $(\log N)^2$. No other changes of keys assignment to peers need to occur.

2.3 TAPESTRY

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I6M7-112012

VOLUME 2 ISSUE 6 November 2012

Allocating the related properties with Pastry[3], Tapestry[4] employs decentralized randomness to achieve both load distribution and routing locality. The difference between Pastry and Tapestry is the handling of network locality and data object replication, and this difference will be more apparent when described in the section on Pasty distributed search technique, with additional mechanisms to provide availability, scalability, and adaptation in the presence of failures and attacks. On the other hand, Tapestry uses multiple roots for each data object to avoid a single point of failure. The resolution of digits from right to left or left to right is arbitrary. A peer's local routing map has multiple levels, where each of them represents a match of the suffix with a digit position in the ID space. To locate the next router, the (n + 1) the level map is examined to locate the entry matching the value of the next digit in the destination ID.

This routing method guarantees that any existing unique peer in the system can be located within at most log BN logical hops, in a system with N peers using Node IDs of base B. Since the peer's local routing map assumes that the preceding digits all match the current peer's suffix, the peer needs only to keep a small constant size (B) entry at each route level, yielding a routing map of fixed constant size - (entries/map) × no. of maps = B × log BN.

2.4 PASTRY

Pastry, like Tapestry, makes use of Paxton-like prefix routing to build a self-organizing decentralized overlay network, where each peer routes client requests and interacts with local instances of one or more applications. Each peer in Pastry is assigned a 128-bit peer identifier known as the Node ID. The Node ID is used to give a peer's position in a circular Node ID space, which ranges from 0 to $2^{128} – 1$. The Node IDs and keys are considered a sequence of digits with base B. Pastry routes messages to the peer whose Node ID is numerically closest to the given key. A peer normally forwards the message to a peer whose Node IDs share with the key a prefix that is at least one digit (or b bits) longer than the prefix that the key shares with the current peer Nod ID.

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I6M7-112012

VOLUME 2 ISSUE 6 November 2012

Following table gives brief overviews of such protocols: CAN, Chord, Pastry and Tapestry [5].

TABLE 2.1 - STRUCTURED P2P NETWORK COMPARISONS

PARAMETER	CAN	CHORD	TAPESTRY	PASTRY
Architecture	Multidimensional ID coordinates space.	Uni directional and circular Node ID space.	Paxton-style global mesh network.	Paxton style global mesh network.
Lookup protocol	{key, value} pairs to map a point P in the coordinate space using uniform hash function.	Matching key and Node ID.	Matching suffix in Node ID.	Matching key and prefix in Node ID.
System Parameters	N-number of peers in network and D-number of dimensions.	N-number of peers in network.	N-number of peers in network and B-base of the chosen peer identifier.	N-number of peers in network and b number of bits (B = 2b) used for the base of the chosen identifier.
Reliability/ Fault resiliency	Failure of peers will not cause network-wide failure. Multiple peers responsible	Failure of peers will not cause network wide failure. Replicate data on multiple	Failure of peers will not cause network-wide failure. Replicate data	Failure of peers will not cause network wide failure. Replicate data

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I6M7-112012

VOLUME 2 ISSUE 6 November 2012

	for each data item. On failures, application retries.	Consecutive peers. On failures, application retries.	across multiple peers. Keep track of multiple paths to each peer.	across multiple peers. Keep track of multiple paths to each peer.
Security	Low level suffers from man-in-middle and Trojan attacks.	Low level suffers from man-in-middle and Trojan attacks.	Low level suffers from man-in-middle and Trojan attacks.	Low level suffers from man-in-middle and Trojan attacks.

2.5 FREENET

Freenet[6] is a completely distributed decentralized peer-to-peer system. It has no notion of global coordination at all. Communication is handled entirely by peers operating at a global level. The system operates as a location-independent distributed file system across many individual computers that allow files to be inserted, stored, and requested anonymously.

A node is simply a computer that is running the Freenet software, and all nodes are treated as equals by the network. Each node maintains its own local data store which it makes available to the network for reading and writing, as well as dynamic routing table containing addresses of other nodes and the keys that they are thought to hold. This removes any single point of failure or control. By following the Freenet protocol, many such nodes spontaneously organize them-selves into an efficient network. The system is designed to respond adaptively to usage patterns, transparently moving, replicating, and deleting files as necessary to provide efficient service without resorting to broadcast searches or centralized location indexes. It is intended that most users of the system will run nodes to -

- Provide security guarantees against inadvertently using a hostile node.

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I6M7-112012

VOLUME 2 ISSUE 6 November 2012

- Increase the storage capacity available to the network as a whole.

The system can be regarded as a cooperative distributed file system incorporating location independence and transparent lazy replication**.** Freenet enables users to share unused disk space, just like systems like distributed.net enable ordinary users to share unused CPU cycles. The system operates at the application layer and assumes the existence of a secure transport layer, although it is transport-independent. It does not seek to provide anonymity for general network usage, only for Freenet file transactions.

2.6 NAPSTER

Napster[7][8] has been described as the trigger application that made peer-to-peer web computing popular. Pre peer-to-peer web applications such as ftp, shared drives, and Windows for workgroups did not have the ease of use, common protocols, standards, and scalability of Napster . Napster hosts act as clients as well as servers for the exchange of music files. A host first joins the network by connecting to a central server known as a broker. Once connected, the host passes information on all the music files it serves to the broker. This information is known as metadata. The broker stores a database of the metadata; this metadata contains the information of all the hosts currently logged into the broker. Clients query the broker's database for particular music files.

The broker replies back with a list of songs and matching peers that contain them. The client can then coordinate with the broker on the exchange of a file from one of the remote hosts. In addition to searching and sharing music, Napster also provides peer-to-peer messaging, chat rooms, and user hot lists. Peer-to-peer messaging allows one peer to talk to another peer. Chat rooms allow groups of users to share information. A message posted to a chat room is seen by all users connected to the chat room. Hot lists contain a list of popular peers with whom a client has been in contact. Peers can add each other to their own hot lists. This hot list will provide information on a peer's metadata, as well as when the peer is online. The broker performs all the coordination of these extra features.

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I6M7-112012

VOLUME 2 ISSUE 6 November 2012

2.7 FASTTRACK

FastTrack[9] is a popular P2P file sharing network. FastTrack is a semi-centralized network, where nodes are classified as ordinary nodes and super nodes. Super node is a higher level node with more responsibilities than an ordinary node. In Gnutella network the same higher level node is called ultra peer. Super nodes act as temporary index servers. Any node with sufficient CPU and network connection can become a super node, and election is done without centralized control. FastTrack is a proprietary protocol, but attempts at cracking the FastTrack protocol have been made but has failed to break the encryption between super nodes.

Some clients have modified participation level at the maximum value for better download performance. This makes the original incentive mechanism useless. Overall download performance is good with multi-source downloading, but system doesn't support sharing partial files. You have to download a file completely before you can upload it. Polluting the network has been quite easy because of UUHash algorithm, which does incomplete file hashes. Today new kzhash should solve the problem, but there is no reliable confirmation about that.

The network has a low amount of legal content, and includes very much fake files. The FastTrack network supports KaZaA[10] and Grokster P2P clients. But now days, Grokster service is down because this service is illegal and unauthorized announced by United States Supreme Court.. KaZaA software is also having legal challenges in the Australia. Future of the FastTrack network existence is not clear. Popularity of a network can be measured on the ground of user volume, but some of those don't have uniform overlay network and the user volume can't be calculated, which is the case with Bit Torrent. User volume has been fluctuated quite much between 2 and 3 million users. It is second in the popularity with 2.6 million users according to. With KaZaA you can download also high quality files bought to you from professional content creators via Altnet. These files are digitally rights managed and are typically offered for use either on a free basis, or on a free-trial basis.

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I6M7-112012

VOLUME 2 ISSUE 6 November 2012

2.8 GNUTELLA

At first Gnutella[11][12] was a decentralized protocol for distributed search on a flat topology of peers. Because the search mechanisms were not scalable and generated unexpected loads on the network, Gnutella has developed to the semi-centralized network implementing Fast Track-like overlay network. Gnutella like Fast Track doesn't have any centralized control point. In Gnutella network nodes are classified as leaf nodes and higher level nodes as ultra peers, which are high capacity nodes that act as proxies for lower capacity nodes. Most popular Gnutella clients are Lime Wire and Shareaza, both are open source software. Lime Wire supports sharing partial files with the partial file sharing option checked, but Gnutella protocol itself doesn't support directly that feature. Like Fast Track there is no mechanism during download to prevent corrupted pieces of a file ruining the whole file. Complete file hashes with Gnutella (SHA-1) can be used for file verification, but only after the download is fully completed. Gnutella has grown to one of the biggest P2P networks and Gnutella is the third biggest with 2.1 million users, data gathered on 22-2-2006.

2.9 BIT TORRENT

BitTorrent[13][14] is a P2P system that uses a central location to manage users' downloads. The central location is a tracker that is contacted when you launch a torrent for file downloading. The tracker keeps track of all the users who have the file (both partially and completely) and connects users to each other for downloading and uploading. BitTorrent supports simultaneous downloading from multiple sources and sharing partially downloaded files, so that a peer can upload a file while still downloading it. "Info hashes" are used to identify files on the network. A torrent file includes a list of piece (block) hashes, which ensures that blocks of the file are always correct and corrupted blocks during download won't ruin the whole download. Corrupted blocks must be re-downloaded. Today most Bit Torrent clients support also tracker less torrents. There is no need for a central tracker with that approach. Tracker less support is done with the help of DHT, which is a layer added on the top of the Bit Torrent network. The Bit Torrent network and DHT portion operate

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I6M7-112012

VOLUME 2 ISSUE 6 November 2012

independently. Each node in the DHT is responsible for indexing a certain percentage of hash files on the network. The first Bit Torrent client to establish a DHT layer was Azureus, followed by the official Bit Torrent client. Although both DHTs are based on Karelia, the two DHT networks are not compatible.

The DHT layer supported by the official client would be known as Mainline DHT network. Azureus client reports 500 000 – 700 000 users on its DHT network. BitTorrent has many clients, for example the original Bit Torrent client, which is open source and written in Python, and BitTornado, which is based on the original client. BitComet is another enhanced client, but is closed source. Azureus is a client with lots of features using Java language. It has also an embedded tracker with password protection, HTTPS and UDP communication support. The network is used for legal content delivery also, for example Linux distributions and game patches. Bit Torrent is a download protocol where peers are connected together by the torrent bases (except DHT), so popularity of overlay network is irrelevant. But Bit Torrent is clearly the most popular regarding download rates; ISPs report very high rates of bandwidth consumption because of Bit Torrent usage. Following table gives brief overviews of such protocols: Freenet, Gnutella, FastTrack/KaZaA and BitTorrent[5].

TABLE 2.2 - A COMPARISON OF VARIOUS UNSTRUCTURED P2P NETWORKS

PARAMETER	Freenet	Gnutella	Fasttrack/KaZaA	Bittorrent
Architecture	Keywords and descriptive text strings to identify data objects.	Flat and ad-hoc network of servants (peers). Flooding request and peers download	Two-level Hierarchical network of Super-Peers and peers.	Peers request information from a central Tracker.

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I6M7-112012

VOLUME 2 ISSUE 6 November 2012

		directly.		
Decentralization	Loosely DHT functionality	Topology is flat With equal peers	No explicit central server. Peers are connected to their Super-Peers.	Centralized model with a Tracker keeping track of peers.
Lookup Protocol	Keys, Descriptive Text String search from peer to peer.	Query flooding.	Super-Peers.	Tracker.
Routing performance	Guarantee to locate data using Key search until the requests Exceeded the Hops-To-Live (HTL) limits.	No guarantee to locate data; improvement made in adapting ultra peer client topologies; good performance for popular content.	Some degree of guarantee to locate data, since queries are routed to the Super-Peers, which has better scaling; good performance for popular content.	Guarantee to locate data and guarantee performance for popular content.
Reliability/ fault resiliency	No hierarchy or central point of failure exists.	Degradation of the performance; peers receive multiple copies	The ordinary peers are reassigned to other Super-Peers.	The Tracker keeps track of the peers and availability of the pieces of files;

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I6M7-112012

VOLUME 2 ISSUE 6 November 2012

		of replies from peers that have the data; requester peers can retry.		avoid choking by fibrillation by changing the peer that is choked once every ten seconds.
Security	Low; suffers from man-in middle and Trojan attacks.	Low; threats - flooding, malicious content, virus spreading, attack on queries, and denial of service attacks.	Low; threats - flooding, malicious or fake content, viruses, etc. Spyware monitors the activities of peers in the background.	Moderate; centralized Tracker manages file transfer and allows more control, which makes it much harder to fake IP addresses, port numbers, etc.
Peers join/leave	Constant.	Constant.	Constant.	Constant.
Routing state	Constant.	Constant.	Constant.	Constant but choking (temporary refusal to upload) may occur.

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I6M7-112012

VOLUME 2 ISSUE 6 November 2012

System parameters	None.	None.	None.	.torrent file.

Table 2.3 - OTHER CHARACTERISTICS OF P2P SYSTEMS

P2P system	Strong points	Weak points
FastTrack	availability, scalability, content lifetime	pollution
Gnutella	availability, scalability, content lifetime	pollution
ED2K	content lifetime, pollution	scalability
Overnet	availability, scalability, content lifetime, pollution	bootstrapping
Bit Torrent (without DHT)	download performance, flash crowd, pollution	availability, scalability, content lifetime

3. NEED FOR SECURITY

In these turbulent times you would think that P2P security would be the least of the world's problems. However corporate fraud and loss of revenue due to attacks on their internal networks has brought P2P to the forefront in the IT world. Napster was the headliner but since its high profile court case more and more P2P applications have been causing the corporate world headaches, which it could do without. With better security protocols this headache could be turned into a valuable asset for the corporate world and for the world[].

3.1 EXTERNAL THREATS

P2P networking allows network to be open to various forms of attack, break-in, espionage, and malicious mischief. P2P doesn't bring any novel threats to the network, just familiar threats such as worms and virus attacks. P2P networks can also allow an employee to

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I6M7-112012

VOLUME 2 ISSUE 6 November 2012

download and use copyrighted material in a way that violates intellectual property laws, and to share files in a manner that violates an organizations security policies. Applications such as Napster, Kazaa, Grokster and others have been popular with music-loving Internet users for several years, and many users take advantage of their employers' high-speed connections to download files at work. This presents numerous problems for the corporate network such as using expensive bandwidth and being subject to a virus attack via an infected file download. Unfortunately, P2P networking avoids enterprise security by providing decentralized security administration, decentralized shared data storage, and a way to circumvent critical perimeter defenses' such as firewalls and NAT devices. If users can install and configure their own P2P clients, all the network managers' server-based security schemes are out the window.

Theft: Companies can lose millions worth of property such as source code due to disguising files using P2P technologies. P2P wrapping tools, such as Wrapstar (a freeware utility can disguise a .zip file, containing company source code, as an MP3 of a music hit. As a result an accomplice outside the company can use Morpheus to download the disguised file. To the companies security this looks like a common transaction, even if the company has frowned upon employees using P2P in music sharing. Little do they know is that their company has just been robbed, and possibly millions worth of software has been lost.

Bandwidth Clogging and File Sharing: P2P applications such as Kazaa, Gnutella and FreeNet make it possible for one computer to share files with another computer located somewhere else on the Internet. A major problem with P2P file-sharing programs is that they result in heavy traffic, which clogs the institution networks. The rich audio and video files that P2P users share are very big. This affects response times for internal users as well as e-business customers and that results in lost income.

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I6M7-112012

VOLUME 2 ISSUE 6 November 2012

Bugs: In order for P2P file-sharing applications to work the appropriate software must be installed on the users system. If this software contains a bug it could expose the network to a number of risks e.g. conflict with business applications or even crash the system.

Encryption Cracking: Distributed processing is another P2P application. Taking lots of desktop computers and adding them together, results in a large amount of computing power to apply to difficult problems. Distributed.Net is a prominent example of this. In 1999 Distributed.Net along with the Electronic Frontier Foundation launched a brute-force attack on the 56-bit DES encryption algorithm. They broke DES in less than 24 hours. Distributed.Net was able to test 245 billion keys per second. At the time DES was the strongest encryption algorithm that the US government allowed for export.

Trojans, Viruses, Sabotage: A user could quite possibly download and install a booby-trapped P2P application that could inflict serious damage. For example a piece of code that looks like a popular IM or file-sharing program could also include a backdoor to allow access to the user's computer. An attacker would then be able to do serious damage or to obtain more information than they should have. P2P software users can easily configure their application to expose confidential information for personal gain. P2P file-sharing applications can result in a loss of control over what data is shared outside the organization. P2P applications get around most security architectures in the same way that a Trojan horse does. The P2P application is installed on a "trusted device" that is allowed to communicate through the corporate firewall with other P2P users. Once the connection is made from the trusted device to the external Internet attackers can gain remote access to the trusted device for the purpose of stealing confidential corporate data, launching a Denial of Service attack or simply gaining control of network resources.

Backdoor Access: P2P applications such as KazaA, Morpheu or Gnutella enable people all over the world to share music, video and software applications. These applications expose data on a user's computer to thousands of people on the Internet. These P2P applications

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I6M7-112012

VOLUME 2 ISSUE 6 November 2012

were not designed for use on corporate networks and as a result introduce serious security vulnerabilities to corporate networked if installed on networked PCs. For example if a user starts Gnutella and then clicks into the corporate Intranet to check their email, an attacker could use this as a backdoor to gain access to the corporate LAN.

Non-encrypted IM: Instant messaging applications like those provided by AOL, Microsoft and Yahoo, also pose an information threat to a company. If these applications are used to discuss sensitive information, an attacker can read all the messages that are sent back and forth across the network or Internet by using a network-monitoring program. IM applications are been developed and enhanced with new capabilities such as voice messaging and file sharing. Adding file sharing to the IM application also adds all of the risks of the file-sharing applications as described previously.

Confidentiality: KaZaA and Gnutella give all clients direct access to files that are stored on a user's hard drive. As a result it is possible for a hacker to find out what operating system the peer computer has and connect to folders that are hidden shares, thus gaining access to folders and information that is confidential.

Authentication: There is also the issue of authentication and authorization. When using P2P you have to be able to determine whether the peer accessing information is who they really say they are and that they access only authorized information.

3.2 INTERNAL THREATS

Along with the external threats previously described there are a few internal issues that have to be dealt with.

Interoperability: Interoperability is a major security concern within P2P networks. The introduction of different platforms, different systems, and different applications working together in a given infrastructure opens a set of security issues we associate with

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I6M7-112012

VOLUME 2 ISSUE 6 November 2012

interoperability. The more differences in a given infrastructure, the more compounded the security problems.

Private Business on a Public Network: Many companies conduct private business on a public network. This leads to an exposure to various security risks. These risks must be addresses in order to avoid the liability this use entails.

Adding and Removing Users: There must be a feasible method to add/delete users to/from the network without increasing vulnerability. The system is under the most threat from users and former users who know the ins and outs of the system e.g. the existence of trapdoors etc.

General Security: P2P shares many security problems and solutions with networks and distributed systems e.g. data tampering, unreliable transport, latency problems, identification problems etc

Distributed Dangers: When using distributed processing applications the user is required to download, install and run an executable file on their workstation in order to participate A denial of service could result if the software is incompatible or if it contains bugs.

The People Problem: There will always be malicious users who are intent on gaining clandestine access to corporate networks. And no matter what security protocols are put in place a skillful attacker, given enough time, will find a way around them. So all that the security buffs need to do is to keep ahead of the hackers by creating bigger and better protocols.

Existing Security standards and techniques in P2P networks: At an alarming rate, people are adopting, in an ad hoc fashion, the tools of the Peer-to-Peer (P2P) revolution. Company files are increasingly made available by being published to the world directly from

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I6M7-112012

VOLUME 2 ISSUE 6 November 2012

a user's PC. Databases, spreadsheets, even entire applications, are becoming enabled with P2P features and critical information is flowing out from every PC. Defending against the threats of ad hoc P2P deployment, and managing or reducing the risks of loss of information or availability of systems requires foresight, planning, and careful selection of the P2P infrastructure upon which your P2P enabled applications and services will be built.

4. SECURE SOCKETS LAYER (SSL) PROTOCOL

For protection of information transmitted over a P2P network, some P2P's employ the industry-standard Secure Sockets Layer (SSL) protocol. This guarantees that files and events sent will arrive unmodified, and unseen, by anyone other than the intended recipient. Moreover, because both peers use SSL both sides automatically prove who they are to each other before any information is transferred over the network. The protocol provides mechanisms to ensure tamperproof, confidential communications with the right counterpart, using the same, well-proven techniques used by all major website operators to protect consumer privacy and financial information transmitted on the Internet.

5. CONCLUSION AND SCOPE OF FUTURE WORK

The fact comes obvious that security is indeed something highly crucial while designing and implementation of P2P Systems. The one and only factor hampering the growth of P2P mechanism is its security. In order to gain the maximum from the P2P Networks, it is important for the users to know the vulnerabilities and the order wherein they are dealt with. As a matter of fact, the biggest merit of P2P Network overlay over contemporary client-server mechanism is that it is a network open and free for all, which means that individual users can now connect to each other without the need of routing through any central server. In any standard network (client- server) the central server is responsible for securing the perimeters and authenticating users thereby blocking unwanted threats and malicious packets. But since in case of P2P Networks, there is no routing through any centralized server, the threat continues to grow. Other benefits of P2P include extensive sharing of files

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I6M7-112012

VOLUME 2 ISSUE 6 November 2012

including music, videos, games and even Instant messaging feasibilities. In order to deal with authentication issues, a mechanism needs to be set up that authorizes only trusted clients to communicate with each other. This can be done by a two way authentication by certificates or keys. These keys can be further be encrypted to provide even more a secure environment in the exchange (similar to that of SSL).

Since P2P deals with extensive clients at a single time, it sometime faces availability issues due to lack of a dedicated server. This can be solved through the construction of a simultaneous distribution and efficiency maintenance protocol over the P2P system. However the main unavoidable aspect comes out to be the careful monitoring of unwanted or malicious traffic from in or outside the network. Usage policies need to be enhanced for better handling of such files and imposition of bare restrictions onto the network distribution overlays. However once secured through encryption, keys and anonymous white collars, some attacks and usage issues can be well dealt with. Moreover enhancement of protocols and redesigning and proper implementation of P2P networks would also do a great deal of favor to the cause. As far as now, the more the use of P2P continues to grow; attacks too continue to become more sophisticated and clever hampering the P2P protocols.

REFERENCES

[1]. S. Ratnasamy, P. Francis, M. Handley, K. Richard , S. Scott, “A Scalable Content Addressable Network”, In Proceeding of SIGCOMM’01, ISSN:0146-4833, Volume 31, Number 4, San Diego, California, USA, pp. 161–172, August 27-31, 2001

[2]. I. Stoica, R. Morris, D. Liben-Nowell, D. R. Karger, M. F. Kaashoek, F. Dabek, H. Balakrishnan, "Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications", IEEE/ACM Transactions on Networking (TON), ISSN:1063-6692, Volume 11, Number 1, pp. 17–32, February 2003

[3]. A. Rowstron and P. Druschel, “Pastry: Scalable, distributed object location and routing for large-scale peer-to-peer systems,” in Proceedings of the Middleware, 2001.

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I6M7-112012

VOLUME 2 ISSUE 6 November 2012

[4]. B. Y. Zhao, L. Huang, J. Stribling, S. C. Rhea, A. D. Joseph, and J. D. Kubiatowicz, "Tapestry: A resilient global-scale overlay for service deployment," IEEE Journal on Selected Areas in Communications, vol. 22, no. 1, pp. 41–53, January 2004.

[5]. E. K. Lua, J. Crowcroft, M. Pias, R. Sharma, and S. Lim. A Survey and Comparison of Peer-to-Peer Overlay Network Schemes. IEEE Communications Survey and Tutorial, March 2004.

[6]. I. Clarke, O. Sandberg, B. Wiley, and T. W. Hong. (1999) Freenet:A distributed anonymous information storage and retrieval system. Freenet White Paper. [Online]. Available: http://freenetproject.org/freenet.pdf

[7]. Napster, accessed via the web: http://www.napster.com.

[8]. Napster Messages, accessed via the web:http://opennap.sourceforge.net/napster.txt" Last Updated - August 6, 2000. Date Viewed - October 6, 2000.

[9]. Fasttrack P2P service provider, accessed via the web: http://www.fasttrack.nu

[10]. N. Leibowitz, M. Ripeanu, and A. Wierzbicki. Deconstructing the KaZaA Network. In 3rd IEEE Workshop on Internet Applications (WIAPP'03), June 2003.

[11]. Gnutella, Accessed via the web: http://www.gnutella.com

[12]. Gnucleus, the Gnutella Web caching system, available - at URL - http - //www.gnucleus.com/gwebcache/

[13]. M. Izal, G. Urvoy-Keller, E. Biersack, P. Felber, A. A. Hamra, and L. Garces-Erice. Dissecting BitTorrent: Five months in a Torrent's Lifetime. In Proceedings of Passive and Active Measurements (PAM) 2004, April 2004.

[14]. J. Pouwelse, P. Garbacki, D. Epema, and H. Sips. A Measurement Study of the BitTorrent Peer-to-Peer File-Sharing System. Technical Report PDS-2004-003, Delft University of Technology, April 2004.

[15]. M Declan, K Jarlath, C. Keith, V. John and O. Dan. P2P Security, Accessed via the web: http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p10.html