PUNE INSTITUTE OF COMPUTER TECHNOLOGY,
DHANKAWADI PUNE-43.

Information and Cyber Security Report
On
Secure Torrent System

SUBMITTED BY

Amey Deshpande	**4224**
Ayush Gupta	**4234**
Krishna Hudge	**4236**

Under The Guidance of
Prof. A.A.Jewalikar

COMPUTER ENGINEERING DEPARTMENT
Academic Year: 2019-20

Secure Torrent System

Contents

List of Figures

Introduction

A distributed system is a network that consists of autonomous computers that are connected using a distribution middleware. They help in sharing different resources and capabilities to provide users with a single and integrated coherent network.

Features of a distributed system are:

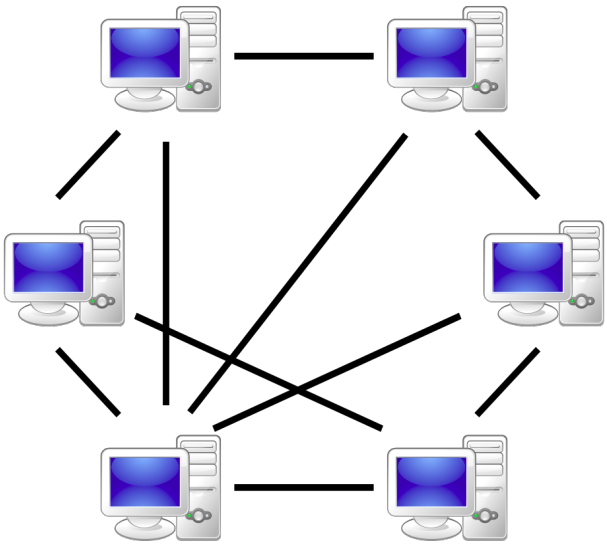
- Components in the system are concurrent. A distributed system allows resource sharing, including software by systems connected to the network at the same time.
- There can be multiple components, but they will generally be autonomous in nature.
- A global clock is not required in a distributed system. The systems can be spread across different geographies.
- Compared to other network models, there is greater fault tolerance in a distributed model.
- Price/performance ratio is much better

Goals of a distributed system include:

- Transparency
- Openness
- Reliability
- Performance
- Scalability

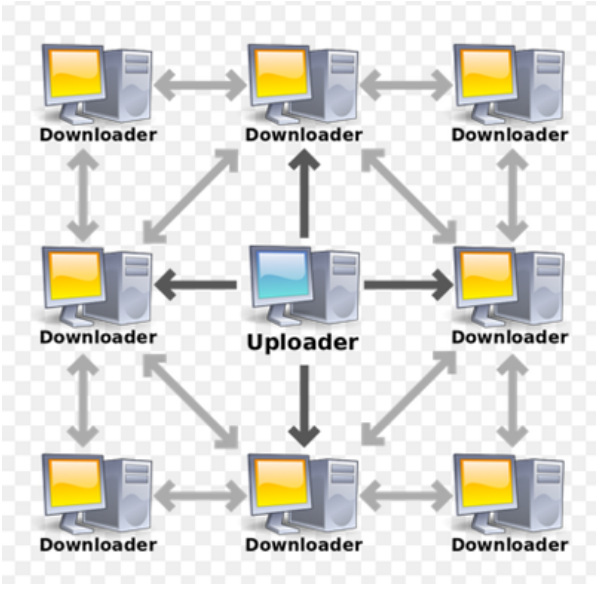
Peer to Peer Network

A peer-to-peer (P2P) network is group of computers, each of which acts as a node for sharing files within the group. Instead of having a central server to act as a shared drive, each computer acts as the server for the files stored upon it. When a P2P network is established over the Internet, a central server can be used to index files, or a distributed network can be established where the sharing of files is split between all the users in the network that are storing a given file.
In the most basic sense, a peer-to-peer network is a simple network where each computer doubles as a node and a server for the files it exclusively holds. These are the same as a home network or office network. However, when P2P networks are established over the internet, the size of the network and the files available allow huge amounts of data to be shared.

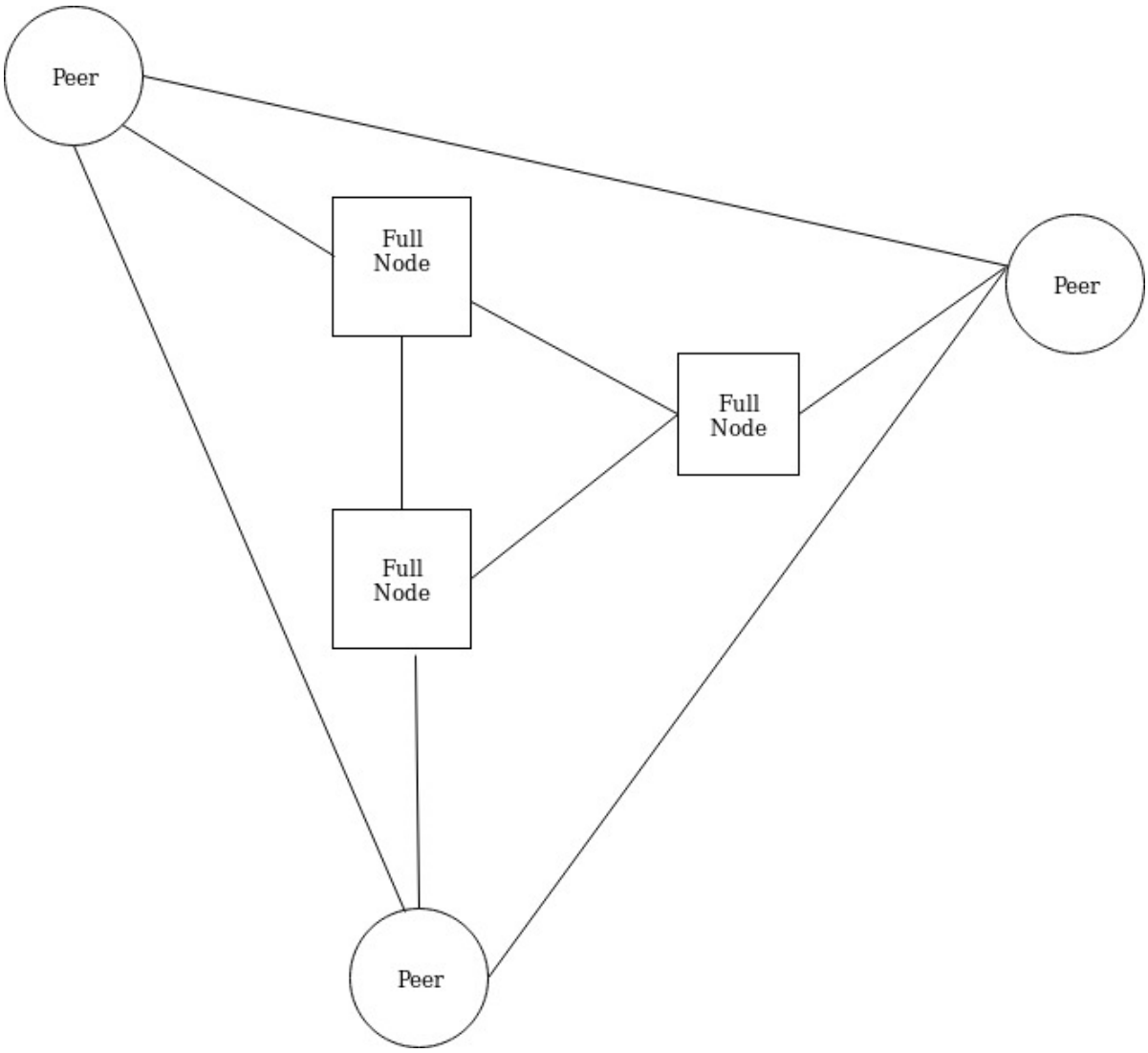


Torrent

The word “torrent” in the tech world, it usually refers to a computer file that contains metadata holding various information. A torrent file normally comes with the extension .torrent but it does not contain the actual contents to be distributed. This information will then be used by a BitTorrent software such as uTorrent, Transmission or BitTorrent for the “real” distribution – which essentially allows for users to easily download torrent files to their personal computers.
In short, a torrent file acts as the key to initiating downloading of the actual content. When someone is interested in receiving a shared file (i.e. books, music, documents, etc.), they must first obtain the corresponding torrent file – by either downloading the .torrent file directly or by using a magnet link.
A BitTorrent software is then required to open this file/link. Once the BitTorrent software scans the torrent file/link, it’ll then need to find the locations of seeders which are sharing the corresponding file. To do so, it will attempt to connect to a list of defined trackers (from the torrent file metadata) and attempt a direct connection. If it’s successful, the appropriate content will then begin transferring.



Architecture



Full Nodes

- Full Nodes contain information about the torrent files and also the peers which have those torrent files.

Peers

-Peers are the computers which are hosting torrent files and also downloading the files from other peers.

Algorithms

0.1 Peer Processing Algorithm

- Get all peers information from full nodes
- Connect to each peer
  - Get torrent info
  - Get how much parts data this peer have
- Store key, value of peer and it parts count (map1).
- create a list for each part containing all peers which have them
- Traverse each part list
  - Select peer which have less value in map1
  - Increase the value of peer in map1
  - Create a thread to get part from that peer

Process

Hosting torrent file

1.)User gives information about the file like name fo file,extension,size
2.)Now the system breaks the file into certain number of parts.
3.)After breaking the file into parts,the system now creates information regarding the torrent file .This information contains name of file,number of parts the file is divided into, extension,file hash.
4.)The torrent file information is now sent to one of the full node.
5.)After receiving the torrent file information ,the full node saves this information in database and broadcasts this information to all other full nodes.This way we are avoiding single point of failure.

Downloading File

1.)User enters the name of the file
2.)The system now requests the one of the full node to give the list of the peers which have the torrent file.
3.)After receiving the list of peers we apply our algorithm of peer processing which we have explained above.
4.)As soon all the parts of the file are received from the peers, they are combined to form the complete file.
5.)This file is now saved in the downloads folder.

Security Risks

Existing torrent system lack the feature of Authentication mechanism for giving access to only verified users. Following are some identified security risks and their solutions.

0.2 No Authentication

Since there is no auth system in place for existing torrent, we added a special node called CA(certificate authority) which checks identity of user.

It uses RSA keys and Challenge Response mechanism.

0.3 Replay Attack

Replay attack can be done during the authorization process that is resolved by limiting the number of correct responses.

0.4 Passive Copy of Files

Since files are transmitted over insecure network we use AES to encrypt files and then transmit that.

Conclusion

We have created a secure distributed peer to peer file sharing network by adding authentication mechanism for giving access to only verified users and reducing the file downloading time using multiple peers.