2. Peer to Peer Network

A Peer to Peer (P2P) network as per definition in [4] is:

Distributed network architecture may be called a Peer-to-Peer (P-to-P, P2P) network, if all the participants on the network share a part of their own resources like bandwidth, processing power, storage capacity and quality, network link capacity, attached printers etc. We see that these shared resources are very much necessary to provide the Service and content offered by their network (e.g. file sharing, shared workspaces etc). The participants of such networks are delegated to provide resource (Service and content) as well as to request (Servant-concept) the resource (Service and content).[4]

Hence a Peer to Peer network architecture is a special scheme of maximum utilization of the available bandwidths by making each participants a client and a server both at the same time and by dividing a big file to a smaller chunks and then distributing them among all participants and let them share resources of each other hence making it one of the most desirable and famous network for big file sharing in a speedy and reliable manner as much as possible. [5]

3. Bit-Torrent Protocol

It is one of the most popular peer-to-peer protocols for file sharing specially of big sizes. A key feature of Bit-Torrent is that files do not transferred sequentially, like in HTTP or FTP but are broken into smaller and fixed-size chunks (*pieces)* and then transferred in parallel making Bit-Torrent transferring the data very quickly and efficiently. To start sharing file with the help of Bit-Torrent, a metadata file which has the information of the chunk(piece) length, values for SHA1 hash of each piece for the integrity, and URL to a "tracker serveris made. Then these metadata files are needed to be hosted on sites like "The Pirate Bay". A peer is a user requesting the file to download and when a peer obtains these metadata files for a desired file, it contacts the "tracker server (a central server to keep track of information list of peers)" to obtain the information of other peers who are already started sharing the same file. The requesting peer will also register itself to the tracker server. The peer finally issues requests for *sub-chunks* (sub-pieces) typically of 16KB, from others. Peers possessing complete file are called "*seeders"* and peers who do not are referred to as "*leechers"*. A leecher establishes communication with another peer by exchanging "*handshake messages"* that consists of a plain-text protocol identifier string, a SHA1 hash that identifies the file(s) that are beingshared, at last a pseudorandom peer identification string. After both peers have exchanged handshake messages, leecher sends a "*bitfield" message*, which contains a bit-array data structure that describes the pieces of the file that the peer has already obtained. After exchanging bitfields message, now the leecher knows which pieces the other peer can supply, and it proceeds by requesting specific chunks. Once a leecher has obtained a piece, it notifies other peers by sending a "*have message"*. [6] To know more about Bit-Torrent protocol the Bit-Torrent protocol specification document can be read. [7]

4. Torrent Poisoning

Torrent poisoning means attacker shares intentionally some specially coded or corrupted data or data having misleading information like file names using the Bit Torrent protocol to secure antipiracy and copyright protection and to gather the IP addresses (source/destination) of the available downloaders (pirates) to trace them back.[8] Following methods are in fashion:

Methods

4.1 Decoy insertion

It is an application of the content poisoning methodology and one of the most popular methods to insert corrupted versions of a particular file into the network. This helps users for finding a corrupted version and so the numbers of its seeders/leechers pair get increased with time rapidly. A malicious user can infect the file by any method like reformatting that will be indistinguishable from the original files for example files with same/similarmetadata. If a malicious user wants to increase the number of users to download the decoys, he may make the corrupted file available via high bandwidth connections. This method will consume a large amount of resources because the malicious server must respond to a large quantity of requests. In result, queries returned are principally corrupted such as anempty (blank) file or executable files infected with a virus. [8]

4.2 Index poisoning

In this method the index of the files are manipulated or altered by the malicious users. The index gives users information to locate the IP addresses of desired content. By index poisoning it become difficult to locate file to peers. The attacker inserts numbers of invalid information into the index of the files to prevent finding the genuine resource. This information (invalid) may contain fake information like (IP addresses, port numbers). In a result whenever a user (peer or node) attempts to download this content corrupted by invalid information, server will fail to establish a connection because of the large volume of the wrong data (invalid information). At this moment users (peers or nodes) will then waste their time trying to establish a connection with the "bogus" users hence increasing the average time it takes to download the file. The index poisoning attack requires lesser resources(bandwidth) and server resources than previously mentioned method of decoy insertion. Furthermore, the index poisoning attacker does not have to transfer files nor he has to respond to the requests. Therefore, index poisoning takes less effort than other methods of attack. [8]

4.3 Spoofing

There are some companies and their primarily work is to disrupt P2P file sharing on behalf of the content providers and they create their own software in order to launch this attack. For example Media-Defender has written their own program which directs users to non-existent locations via fake or bogus search outputs and because users typically select one of the top four to six search results only the idea

behind this is that most of the normal users will simply give up their search attempts because of the frustration that they got. [8]

4.4 Interdiction

In this method of attack it prevents distributors from serving the users and thus slowing down the P2P file sharing. The interdiction attacker's servers will constantly connect to the destined file, which floods the upstream bandwidth of the providers and ultimately prevents other users from downloading the file. [8]

4.5 Selective content poisoning

Selective content poisoning (also known as proactive or discriminatory content poisoning) tries to detect the pirates while allowing the legitimate ones to continue to enjoy the services provided by an open Peer to Peer network. This protocol identifies a peer (node or user) with its initiating address while theformat of the index of the file is made change incorporating a digital signature. When A peer starts downloading or uploading of the files the peer (node) authentication protocol can then establish how legitimate is a peer now. Using signatures based on identity, the proposed system is expected to enable each peer to identify pirates with no need for communication with a central authority. The selective content poisoning protocol then sends poisoned data (chunks) to detected pirates only who are now requesting the copyright protected file. If all genuine legitimate users of P2P simply deny the download requests from most of the famous pirates, then pirates could usually accumulate the clean data (chunks) from the colluders (who are the paid peers and who share downloaded content with others without the authorization). However, we observe that this method of the selective content poisoning forces the pirates more to discard even clean chunks, hence prolonging their download time. [8]

4.6 Uncooperative-peer attack

In this attack, the attacker will join the targeted swarm and establishes connections with many peers as possible. However, the attacker will never provide any data (chunks) which is authentic or otherwise to the peers. A common version of this attack is the "chatty peer" attack. Now attacker establishes the connection with the targetwith the help of the handshake message, showing off that they have a plenty of available data (chunks). Attacker never provides any (data) chunks, but resends repeatedly the handshake and message. The peer will wastehis time with attacker, without downloading chunks (piece) from others hence these attacks essentially will prevent the download.[8]

5. Counter Measures

All of the above methods of attack that have been described so far are not effective on their own particularly, as for each of them effective countermeasures have been evolved. If these measures combinethey willmake a significant impact on illegal P-2-P file sharing using Bit Torrent protocols and Torrent files.

- Bit Torrent is highly resistant to content poisoning in comparison to the index poisoning, because it has ability to verify and cross-check individual file data (chunks). Overall, Bit Torrent is one of the most resistant P2P file sharing methods to poisoning.
- Bit Torrent users if they are the members of any Private Tracker websites (where one has to be a member of the Torrent tracker sites) if poisonedthentorrents can be labeled easily and can be deleted and the person responsible can be banned from the site(s) forever.
- Public torrent tracker sites now have enabled the options to report if a torrent has been poisoned (fake or malicious). Therefor torrent files that are going to be shared by public trackers can have the same type of the levels of quality assurance as Private Tracker websites.
- Tracker technology as well as Bit Torrent client programs have improved over time, and many kinds of spoofing that were possible in the past are no longer possible.
- Whether public or private, tracker websites now have been selectively jumped over to using ofSHTTP to distribute their web text and image content. By using SHTTP for the website content (versus tracker communications) many poisoning techniques will be rendered impossible.

6. Anonymity

With an increasing number of Bit Torrent users seeking solutions to hide their identities (privacy) from the external world, secure privacy services have seen a growth innumbers of the customer recently. We are listing below some of the most well used services that allow Bit Torrent users to hide their IP-addresses from the public and get a better sense of security (anonymity). The services discussed in this post range from totally free to costing several dollars per month. Now it is found that generally free services are slower or have other restrictions, and paid services will provide the same speeds as your normal regular connection would. [9]

6.1 VPN

VPN is one of the bestways to ensure privacy while using Bit Torrent. At cost of a few dollars/month a VPNs can route all your traffic through their very own servers, andthus can hides yourIP addressfrom the others. Some of the VPNs offer a free plan also, but these are significantly not onlyslower but also are not really suited to Bit Torrent users who demand more. Unlike the all other services listed in this paper, VPNs are not only limited to just Bit Torrent traffic, but they will also conceal the source of all other traffic on your connection. [9]

6.2 BT Guard

BT Guard is a proxy service that hides the IP-addresses of its users from the public view. The service works on almost all(Windows, Mac, Linux) operating system. It is developed keeping Bit Torrent users in mind. While using the already configured client, users also have an option to set up their own client to work with BT Guard. Torrent Privacy is another proxy service that is very similar to that of BTGuard.[9]

6.3 Seed box

A seed box is a Bit Torrent jargon for a dedicated high-speed server, which is used exclusively for torrent transfers. With the help of a seed box (tools and protocol), users generally get very high download speeds and their IP-addresses are not shared with any other person or system. When a download got finished users can download the files to their PC through a fast http service.[9]

6.4 TOR Networks

Tor network is being the more and more popular overlay network in fashion for anonymous TCP-based applications. Tor provides a stronger sense of anonymity than the proxy server approach because it operates around a decentralized design; therefore, no single entity knows both information together at any time, the source and the destination of an anonymous flow. It is important to note that only the first Tor router on the path (called the *entry guard*) knows the true identity of the "requester" client, and only the last one (Tor router) on the path (called the *exitrouter*) knows the identity of the destination server. Tor provides a strong degree of anonymity, subject to the assumption that it is difficult for a single entity to control both the first and last Tor routers on a user's virtual circuit. Only an ISP or group of colluding ISPs *could* feasibly monitor the entering and exiting links from and to Tor network and could perform traffic analysis to link the clients and the destinations pairs. [10]

7. Conclusion

While comparing the various attacks used to support antipiracy and the methods involved to sustain anonymity one can apply enforcement to protect his copyrighted work but none of them have been proven most efficient as there are countermeasures of torrent protocols but lot of work is still going on in this direction and a global framework is desirable. So these methods and techniques are giving a greater help to Cyber Law and Enforcement Agencies to enforce the legality to the use of antipiracy. Although it is clear that the torrent software are not illegal as they are very useful in information and data sharing but pirating the copyrighted materials over these networks are illegal.

References

[1] http://en.wikipedia.org/wiki/Peer-to-peer.
[2] http://en.wikipedia.org/wiki/BitTorrent.
[3] Jungjae Lee and Jongweon Kim "**Piracy Tracking System of the BitTorrent"** International Journal of Security and Its Applications Vol.7, No.6 (2013), pp.191-198 http://dx.doi.org/10.14257/ijsia.2013.7.6.20
[4] J.A. Pouwelse, P. Garbacki, D.H.J. Epema and H.J. Sips. *A Measurement Study of the BitTorrent Peer-to-Peer File-Sharing System*. Delft University of Technology. http://www.pds.ewi.tudelft.nl/reports/2004/PDS-2004-003/
[5] "Peer-to-peer networking with BitTorrent" by Jahn Arne Johnsenjahnarne@stud.ntnu.no, Lars Erik Karlsen*larserka@stud.ntnu.no*,Sebjørn SætherBirkeland*sebjorns@stud.ntnu.no*
[6] **"**The challenges of Stopping Illegal Peer-to-Peer File Sharing **"**Kevin Bauer, Dirk Grunwald, and Douglas Sicker, Department of Computer Science, University of Colorado.
[7] BitTorrent protocol specification. http://wiki.theory.org/BitTorrentSpecification.
[8] http://en.wikipedia.org/wiki/Torrent_poisoning
[9] https://torrentfreak.com/5-ways-to-download-torrents-anonymously/2/
[10] THE CHALLENGES OF STOPPING ILLEGAL PEER-TO-PEER FILE SHARING, Kevin Bauer, Dirk Grunwald, and Douglas Sicker Department of Computer Science, University of Colorado