Indian Journal of Science and Technology Vol. 5 No. 7 (July 2012) ISSN: 0974- 6846

A novel approach for mitigating Distributed Denial of Service attacks drawn on bit-torrent protocol in computer networks

S. S. Nagamuthu Krishnan[1*] and V. Saravanan[2]
[1]*Thiagarajar School of Management, Madurai, Tamilnadu, Bhartathiar University, Coimbatore - 641 046*
[2]*Department of Computer Applications, Sri Venkateswara College of Computer Applications and Management, Coimbatore-641105, India*
ssnkrishnan@gmail.com*, tvsaran@hotmail.com

Abstract
The objective of the paper is to propose and describe a possible defense mechanism that can be taken up to prevent exploitation of Bit torrent in a peer-to-peer network.

Keywords: Bit torrent, Torrent, Lechers, Seeds, Tracker.

Introduction Peer-to-peer networks are popular in transferring large files over the internet, particularly to store music (e.g. Napster) in the beginning. A Centralized server maintains current client information, including the files that they make available at a point.

A true peer-to-peer network does not require centralized severs, but requires the client to know only the address of remote peer to bootstrap its connection to the network, thereby identifying the other peers' identity by means of querying the peers (Castro *et al.,* 2002).

The next advancement in peer-to-peer sharing is the introduction of supernode (Giuli *et al.,* 2005) based architecture wherein a supernode acts as a directory server for other lower powered clients achieving increased scalability.

A most successful and efficient protocol for sharing files over the internet is the Bit-torrent, due to its file centered design and fairness mechanism for rewarding up sharing users (http://www.what-is-torrent.com/, 2002).

A Serious vulnerability in Bit-Torrent protocol could be the usage of tracker a coordinating centralized server element for a swarm (ad-hoc file sharing network) (Kaucheuing, 2003). The tracker is specified by the distributor, and all the peers in the swarm trust the tracker without making any authentication or verification. Hence, the distributor could even deploy a modified tracker that provides malicious coordination data; that may direct the traffic to an arbitrary machine in a service port.

A potential attack exploiting the vulnerability mentioned above and using the members of the swarmin abit-torrent protocol applied in a swarm could be to launch an application level Distributed Denial of Service (DDoS) attack (Giovanni Branca, 2004). This kind of attack does not require any modification in client side software and it can be directly implemented in the Bit-torrent world by initiating DDoS traffic from innocent users within a swarm. This kind of attack, an easy to implement and hard to defend makes a TCP connection to an arbitrary port, and can be adapted to a variety of services as HTTP and SMTP.

Bit-Torrent

Bit-Torrent was originally developed by Bram Cohen (Incentives Build Robustness in BitTorrent. http://www.bittorrent.org/bittorrentecon.pdf). It is different from earlier protocols in the way it forms smaller ad-hoc networks called as swarms for transfer of a file or set of files between peers. The tracker or the centralized server is informed about the presence of members, making it to maintain and distribute to peers a list of currently connected peers.

For enabling transfer among a group of users the Bit-Torrent tracker software should be running in a server in the original distributor. A torrent file containing the URL of tracker with its payload divided into separately hashed chunks, registered with the tracker should be available with the distributor.

Now the distributor launches a client and loads the previously created torrent files and directs the client towards it and from there-on they can be offered to potential downloader. The client reads the tracker URL while downloading the torrent file and intimates its presence to the tracker and the tracker records the IP (http://thepiratebay.org) of the new peer with a time stamp for time last checked to the database. The tracker also responds the client with a list of addresses of other clients in the swarm and also the information that whether each client possesses the torrent file in its entirety or not.

Then, the Bit-Torrent client gathers in parallel chunks from its peers by contacting them through their addresses and compares the calculated checksum with the actual checksum for ensuring correctness of chunks. So, data transfer occurs in parallel from one client to many active members in the swarm at same time. Thus, Bit-Torrent proves to be an economic means of file distribution for files in high demand than the traditional Client/Server model (http://www.mininova.org/, 2004).

The client also announces its continued participation in the swarm with the tracker and receives an updated list of peers each time and finally when it receives and checks all the chunks it announces itself as a seed(a node that possess a file in its entirety).

As Fig.1 (Wiki, 2003) illustrates there can be separate control connection with the tracker, and independent data connections among peers, thus enabling them to download chunks from any combination of peers in the swarm.

Indian Journal of Science and Technology Vol. 5 No. 7 (July 2012) ISSN: 0974- 6846

Fig. 1. Bit-Torrent

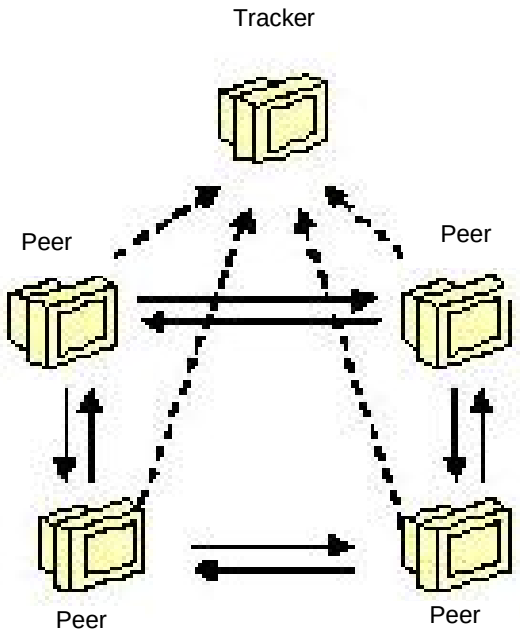
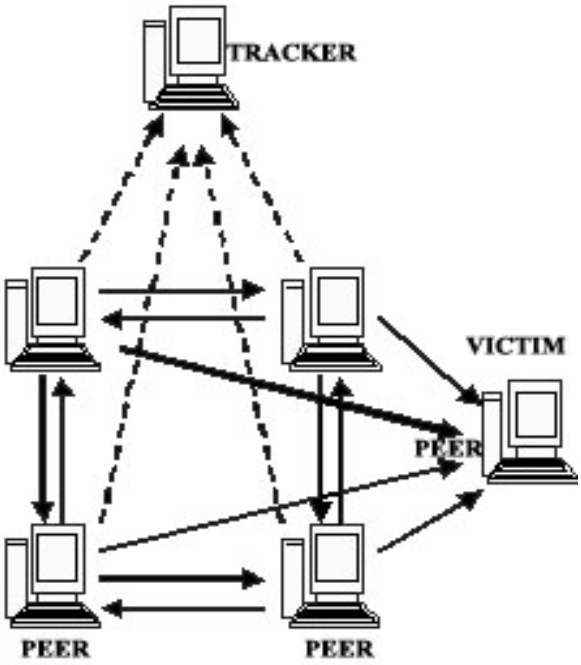


Fig. 2. DDOS attack Scenario



Bit-Torrent gets its application in many legal purposes such as distribution of Linux ISO images (http://www.wired.com/wired/archive/13.01/bittorrent.html, 2003) and software for an online multi player role playing game. It has also become massively popular in piracy community for transfer of music, movies and television shows as shown in Fig.1.

Vulnerability in BitTorrent

Torrents are files that contain the information about the file to be downloaded. The torrent can be created by any one thus possessing a danger of creating bogus records and directing the swarm towards a victim in order to perform the DDoS attack (http://www.utorrent.com/documentation/make-a-torrent).

A tracker server is one that assists peer communication applying the Bit-Torrent protocol, and the clients communicate with the tracker for initiating downloads and get updated peer information. There are two kinds of trackers viz. open tracker and private tracker (http://thepiratebay.org). These trackers have a great chance of being manipulated and disguising the victim to be a file provider. This possesses a greater danger for the P2P network to be attacked.

In this paper, as an improvement to the earlier approaches towards mitigating DDoS attacks in using BitTorrent for file transfer/download, the validity of the torrent file is checked by monitoring the download rate and status, and if found bogus the trace of it will be removed thereby preventing the file provider becoming a victim of the attack, and new users will not also approach the file provider as the trace of the torrent file is not available to enable tracing of path to the file provider. Also, a measure is taken for monitoring the percentage of download, and a peer to flood the feedback about the status of download to the tracker and other peers that are desired on a file available with a file provider as pointed out in Fig.2.

Related Work

A P2P network with millions of peers involved possess a potential risk of serving as a DDoS engine targeting a host. A study was made on query flood attacks in Gneutella (Daswani *et al.,* 2002) and it examines the case when the target is Gneutella Peer. Here the focus is on attacks in arbitrary hosts.

Two attack approaches described by another work (Naoumov & Ross, 2006) are poisoning the distributed index and peers' routing tables, wherein both of them the targeted host could be a web server, mail server or an user's desktop, that doesn't even participate in the P2P system (Naoumov & Ross, 2006). The attacks have been examined in Overnet a popular DHT based file sharing system, wherein DDoS attacks on a targeted host can be created very easily by using short duration limited poisoning attacks.

Routing poisoning (Naoumov & Ross, 2006) tricks peers to add bogus neighbors to the routing tables with the IP address of the victim and attempts to poison the routing table of the P2P nodes, thus making the target node an overlay neighbor of many other peers in the system and enabling the multitude of peers to flood messages of query, publish or overlay maintenance to the target, and if the poisoning is repeated on many peers the victim host might receive millions of flooding messages and it reply with error message for each message received thus clogging the outward stream pipe of the victim, functioning similar to reflector attacks.

Indian Journal of Science and Technology Vol. 5 No. 7 (July 2012) ISSN: 0974- 6846

Index poisoning (Naoumov & Ross, 2006) attack is inserting bogus records indicating one or more popular files to be located in the target IP address or port no. into the P2P index system. The Index maps file identifiers to locations and the goal of attack is to trick indexing peers in adding bogus records for local indices, and they happen to be the IP address and port number of victim host. After the poisoning process the peers contacting the victim host might attempt to download the file from the port specified in bogus record, and the victim might ignore this message and close TCP connection or it might hang and result in TCP connection DDoS attack exhausting victim's resources, if the process is repeated by several hosts, and could not be managed by cookies. Also, when the peers search for popular files the index indicate the target location that could be a mail or web server or an user's desktop and the peers connect to the target for downloading files, thus overwhelming it with a set of open TCP connections that prevent legitimate users from having services. A countermeasure on routing poisoning and index poisoning, with a minor amplification factor check the existence of a victim host and another was to employ encryption and closed source software and implement handshake introducing additional overhead.

There had been many other attempts to secure P2P network for normal functioning during attacks particularly for correct message delivery, fault isolation, and denial of service defense. The present proposal in this paper is a defense mechanism to prevent large scale DDoS attacks to other targets, and not the P2P network itself. Three different mechanisms are used to keep the Bit-Torrent protocol secure from DDoS attacks, thus effecting prevention, detection and recovery from DDoS attacks.

Proposed defense mechanisms

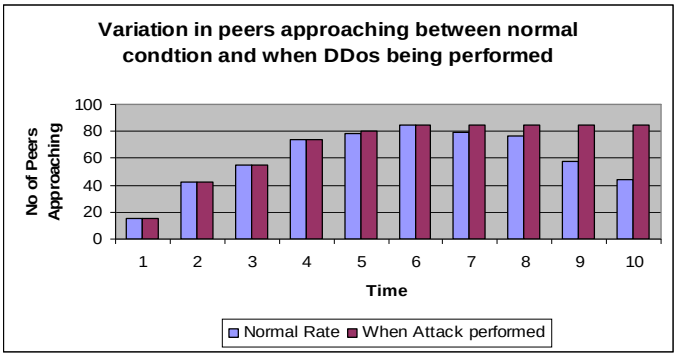
In this paper the vulnerability in Bit-Torrent protocol (http://en.wikipedia.org/wiki/Fasttrack, 2003) is highlighted and possible methods are proposed as defense mechanisms. In the Bit Torrent when a file provider is ready to share a file, he releases a torrent file to be used by others. When the peer starts using it they will be approaching the file provider. The number of peers approaching will be increasing gradually with respect to time. This is clearly shown in Graph 1.

As per the simulation observation, rise in the number of peers approaching is almost 20 peers for an hour. Thus the number of peers approaching will be considerably increasing with respect to time. After a particular time when almost all the peers that were downloading a file has some percentage of that file, they themselves become a seed to other peers whose are also interested in the current file, thus reducing the number of peers approaching the current file provider automatically.

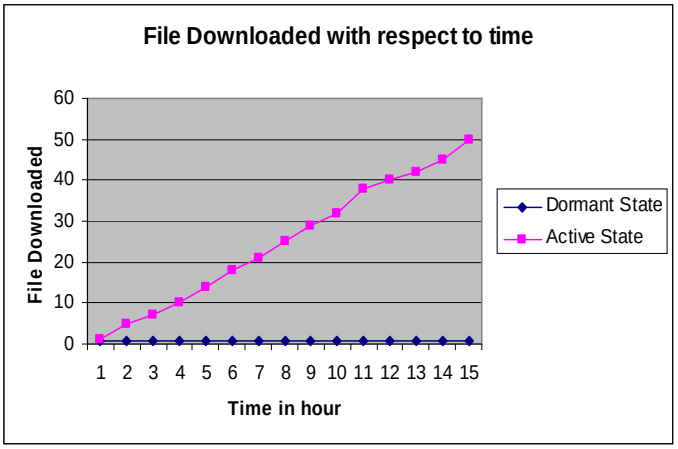
Thus if there is a reduction in the number of peers approaching, definitely the bandwidth of the network is freed and the file providers' network bandwidth attains a normal state. Hence in order to perform a DDoS attack in this case there should be a constant increase in the number of peers approaching, as the time increases. This keeps the bandwidth of the network very busy. As the peers approaching the file provider keeps on increasing, at a particular point the entire bandwidth to the system is blocked and hence the system is said to be under the state of DDoS attack. The graph below shows the difference in the rate of increase in the number of peers approaching the file provider with respect to time between the file transfer under normal condition and when the victim is under attack.

Defense mechanisms

Graph1. Variation in of number peers approaching during DDoS attacks



Graph 2. The downloading status



Bit-Torrent traffic had been reported to contribute to 30% of the Internet traffic now-a-days and the number of participants has been growing rapidly. For such a protocol that is significantly involved in the Internet traffic, the robustness and security must be evaluated carefully.

Torrent files are added to the tracker with a unique Hash ID. These hash IDs can be used to identify the particular torrent. When a peer uses a torrent file to download a file, the peer's downloading rate and the status of the download should always be monitored. With reference to the simulation study interpretation shown above in *Graph 1* we can come to a conclusion that the

Indian Journal of Science and Technology Vol. 5 No. 7 (July 2012) ISSN: 0974- 6846

percentage of file downloaded should be proportional to the increase in time. Hence when a torrent file is being used and the download is being initiated, there should be a constant increase in the percentage of the file that is downloaded.

Table 1.Bandwidth Improvement in victim's side due to flooding of feedback

Time (hr)	Percentage of bandwidth Occupied(Proposed method)(MBPS)	Percentage of bandwidth Occupied(Existing) (MBPS)
0.2	60	60
0.4	50	58
0.6	45	55
0.8	40	52
1	20	50
1.2	0	45

Table 2.Withdrawal of hosts from the victim due to flooding feedback

Time (hr)	No of hosts contacting the victim(Proposed)	No of hosts contacting the victim(Existing)
0.2	1200	1200
0.4	1000	1160
0.6	900	1100
0.8	800	1040
1	400	1000
1.2	0	900

Here, in the proposed method the download rate and the status is monitored, and if the downloading state is said to be active, the torrent file that is being used is said to be a valid one, and the file provider is said to have a file of our desire. If in case, the downloading status is said to be dormant for a long period of time, the peer will not take any action and the downloading progress will be dormant. This will be the status for all the peers that are approaching the seed.

In this scenario the peer that is already in dormant state will still be in tact with the seed, and in addition to it new lecher's will be approaching the file providers leading to distributed denial of service. Hence in this case there is a maximum possibility of the file provider being attacked shortly. In order to prevent the DDoS attack we should avoid further approach of the peers to the file provider. Thus to prevent the situation from becoming worse we use the peer that first approaches the file provider to pass a message to the tracker of its concern to remove the trace of the torrent with the mentioned hash id. By doing so the bogus torrent will be removed and any new user will be prevented from use of that torrent, as there will not be any trace to the file provider (victim). The *Graph 2* shows the downloading states active and dormant. The dormant state of lechers can be tolerated not more than 15 min, as per the observation.

Flooding of feedback to all the peers

In the above mentioned method the hash id of the bogus torrent will be removed, thereby preventing the new users from approaching the victim. But the one that has already approached will still be there blocking the bandwidth of the victim. In the flooding feedback concept the peer that approaches the file provider first, after waiting for a long time passes a feedback not only to the tracker but also to all the peers that are actively participating in the downloading process. This process facilitates to inform the torrent client to stop the process of download for the torrent with the mentioned hash id, thereby all the peers will be withdrawn from the victim thus freeing the bandwidth of the victim and keeping it free from attack.

Table 1 shows a comparison of results of simulation done with a sample number of P2P nodes, between the proposed method and existing method towards relieving the bandwidth of victim. It clearly indicates that as time passes by, and as the feedback is passed to the peers participating in the download, the percentage of bandwidth occupied at the victim's end shows a phenomenal reduction resulting in freeing of bandwidth at a stage, which the node can use productively. *Table 2* is also an indication of improvement or reduction in the number of hosts contacting the victim node, as the feedback reaches them. At a point in time the number of nodes gets reduced to absolute zero, or the victim is totally relieved, which is a substantial increase in benefit over the existing method in allowing legitimate users to have the service of the affected node.

Monitoring the percentage of download

When a peer uses a torrent file to download the file it approaches the tracker, and it directs the peer to the file provider. When the download is being initiated, starting from the beginning, the peer informs about its status to tracker till it completes the download. Hence, we can employ this new method in a better way than the existing method. In this method any peer before it starts the download confirms with the tracker of each and every peer that is using the torrent file. If the process is active, the new download will begin, else if the state is said to be dormant the download will not be initiated.

Conclusion

With the rise in the security there has always been a rise in the threat to networks. The attackers keenly watch over the networks for vulnerabilities in the network to perform one or the other attacks. The proposed defense mechanisms concentrate on limiting a category of DDoS attack drawn on Bit Torrent affecting the bandwidth of the victim both by passing information to the tracker and the peers involved in download, and initiating a download by monitoring the percentage of download with the tracker of each and every peer for a particular file of interest.

Future Enhancement

The defense mechanisms proposed are almost the measures that can be used to prevent the impact of attack getting worse. Thus it would be better if there is a method that could be used to prevent the attack well in advance. A future enhancement could be, employing a proper authentication and verification for the entire torrent

Indian Journal of Science and Technology Vol. 5 No. 7 (July 2012) ISSN: 0974- 6846

files distributed all over the internet and ones that are being posted over the internet. A special enhancement can also be employed to the torrent client software to validate and verify the torrent that is to be used well in advance, thus preventing the DDoS attack well before it is performed.

Acknowledgement

We thank Mr. M Srinivasan, Faculty member, Thiagarajar School of Management, Madurai, Tamilnadu, India; V. Arun Kumar, C. Kappilan, S. Rajarathinam, S. Vignesh, T. Karthick,V. Arun Kumar, Thiagarajar School of Management, Madurai, Tamilnadu, India.

References

1. Castro M, Druschel P, Ganesh A, Rowstron A and Wallach DS (2002) Security for structured peer-to-peer overlay networks. *In OSDI.*
2. Daswani N and Garcia-MolinaH (2002) Query-flood DoS attacks in Gnutella. *CCS 2002.*
3. Naoum Naoumov and Keith Ross (2006) Exploiting P2P systems for DDoS Attacks. INFOSCALE '06. *Proce. First Intl. Conf. Scalable Info. Sys.,* May 29-June 1, Hong Kong © .
4. Giuli TJ, Maniatis, Roussopoulos M, Baker M, Rosenthal DS and Roussopoulos M (2005) Attrition defenses for a peer-to-peer digital preservation system. *Proc. USENIX Technical Conf.*