International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 6 Issue: 1 01 – 05

Black Hole Attack, in P2P based VoD Service, and its Effects on Swarm Sizes and Seeders

Sudipta Majumder
Dept of CSE, Dept. of ECE
DUIET, Dibrugarh University
Assam,India
Email:Sudipta2020@gmail.com

Md. Anwar Hussain
NERIST
Arunachal Pradesh,India
Email: bubuli_99@yahoo.com

Abstract: From the inception, BitTorrent has been under several types of attacks. Most of these attacks were aimed to deteriorate the performance of BitTorrent network or to collapse it.In this paper we have presented the effect of Black-hole attack especially in the case of BitTorrent based VoD services .we have simulated black-hole attack for BitTorrent based VoD services and studied the effect of number of malicious nodes in peer network of various swarm sizes. The number of attacking nodes taken was 1, 2, and 3 whereas the size of swarms was 10, 20 and 30. Also another important parameter taken into consideration for studying the effect was then total number of seeders. We have taken observation for attack simulations for various scenarios depending upon swarm size, numbers of seeder and number of attack nodes.

Keywords: *Black hole attack, seeders, swarm, tracker, leecher, BitTorrent, Video-on demand, peer to peer network,throughput,first chunk download time, last chunk download finish time*

*****

I. INTRODUCTION

A Peer- to- Peer (P2P) network is a distributed system. In such type of network, nodes participating in the network exchange data without any centralized server or control. There are no dedicated servers in peer-based networks like P2P networks. Here all nodes act as both clients and servers. The main characteristics of the P2P network are that it creates a self-organizing virtual topology on top of the Internet. This virtual topology is also referred to as the P2P overlay network or P2P logical network.

A P2P overlay network acts as an application layer application.it works on the top of the Internet Protocol (IP) networks. Also, the self-organizing topology of the P2P network does not represent the underlying physical topology of the physical network. A host or node which participates in the networks are known as peers.P2P based networks are different from traditional client-server architecture because every peer can act as both a server and a client. Therefore, in most circumstances, the role of every peer in a P2P network is symmetric. Because of this symmetry in roles, P2P systems can offer services beyond the client-server systems. These services include building self - organizing overlay network, trust between peers, redundant storage, resource sharing and searching between peers, load balancing, selection of nearby peers, robust routing architecture, and massive scalability[1]. There are many applications that run on P2P based networks. While the most popular practical and prominent application of P2P network is the file sharing and Video on demand services. Besides this, there are other applications are available such as live telecasting, video conferencing etc. Infect, Skype also work on this principle.

II. VIDEO ON DEMAND SERVICES

Video on demand services is one of the widely used services now a day. And it has huge potential in terms of revenue generation and ease of service. The consumer can, as per his/ her wish, can demand any video-based service at any video anytime. If any user uses VoD service then he need not depend on the content provider for availing the services. He can get the requested video from its peers who have parts of the video. Thus it provides more flexibility and convenience. Such Video-on-demand (VoD) systems are made in such a way that is capable of delivering the requested Video cautiously to the user. Unlike live streaming, there is complete control over the media, in VoD systems. It also has operations such as pause, forward and backward functionalities. The characteristic behavior of VoD systems is that it should be able to handle a large number of video demands made by users. Here users are usually requesting for videos asynchronously for watching different parts of the same video at any given time[3].

The practical implementation of the VoD system with the behavior of scalability and quality is very challenging. It becomescucumber some especially when the consumers requires videos exactly in the same order as the video would play.In this kind of systems,large videos are required to be broken into many

small blocks of pieces. Both the system throughput and the rate, at which the content can be distributed to users, greatly depend on the diversity of the blocks contained at different peers. The challenge of providing VoD services networks lies in the fact that the blocks have to be received at the peer side in a sequential order, and time constraints have to be considered at all times to guarantee continuous visualization. Hence VoD services using mesh-based P2P can effectively address all the issues related to the efficient Video-on-demand (VoD) services[4].

III. BITTORRENT:

BitTorrent architecture usually consists of the following:

a. A tracker which keeps track of the files or chunks of the large video file.
b. A Seed which a normal peer but it is the original downloader of the file.
c. Staticmeta information about how to download a file. It is normally called torrent file.
d. The end users which are supposed to download the file. They are also called “leecher”.

In order to public a file using BitTorrent based VoD services; creation of Meta info is required. This Meta info is also referred as torrent file. The torrent file contains the filename, size, hashing information and the URL of the “tracker”. If any user needs to download a file, he needs to find the torrent file associated with that file. The torrent file is published to the internet in normal ways so that it is accessible to the users[5].

The main purpose of a tracker is to keep track or log of peers that are currently downloading a file, and also it assists peers to find other peers. The tracker does not save a copy of data for themselves nor is it directly involved in data transmission. The tracker and the downloading users exchange information using a simple protocol on top of HTTP. First, the user gives information to the tracker about which file it’s downloading, ports it’s listening on etc. The response from the tracker is a list of other users which are downloading the same file and information on how to contact them. This group of peers that all share the same torrent represents a ‘swarm’ [6].

IV. BLACK HOLE ATTACK ON BITTORRENT BASED VOD SERVICES.

The Black Hole is a type of Attack where malicious nodes never send true control messages initially [2]. Also it publishes a false torrent file of a rare file. To carry out a black hole attack, malicious node waits for neighboring nodes to send REQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination through itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets through the malicious node. Malicious node attacks all RREQ messages from other source nodes al so and takes over all routes. Therefore all packets are sent to a point when they are not forwardedanywhere [7].

V. BITTORRENT ATTACK SIMULATION AND RESULT ANALYSIS

Here we have simulated the black hole attack with many swarm sizes.The sizes of Swarm taken are 10,20 and 30. The number of the number of malicious nodesis1, 2 and 3. The number of malicious attacks node vary from 1 to 3 for various numbers of seeders for each swarm size.

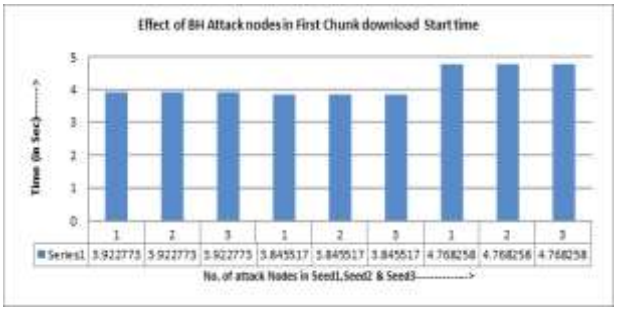

Figure 1: Effect of BH Attack nodes in First Chunk download Start time

From the figure 1, we can see the effect of Black Hole attack nodes in the first chunk download Star in the given figure the y-axisrepresent time in seconds. Thex-axis represents the effect of Black Hole notes on different swarm sizes.From the figure, we can conclude that number of attack nodes doesn't affect the overall performance of the swamp by very large extent the effect of attack nodes on Swarm sizes of 10 and 20 are almost similar but the effect of attack nodes are prominent in swamp size of 30. this is because large Swarm sized network has more number of communication among themselves thus it gives an opportunity to the attacking notes to take participate in the communication among the participating peers.

Some important parameters for measuring the quality of service by the VoD service provider can be summarized as follows:How much time it takes for starting downloading of desired content after requesting the service . i.e. First chunk download start time.

1. How much time it takes to start playing the video after requesting the service . i.e first chunk download finish time.

ISSN: 2321-8169
01 – 05

2. How much time it takes to finish downloading of the whole video after Requesting theservice.i.e last chunk download finish time. If last chunkdownload finish time is very large then it may cause service degradation

In figure1, we have observed that the black hole attack simulations have no impact on the first chunk download time. Even if we increase the number of attack nodes irrespective numbers of seeds, it has no effect.Thus,we can conclude that the number of attacking notes doesn't affect the service start time since it is not affecting first chunk download time but the case is very different for first trunk download time

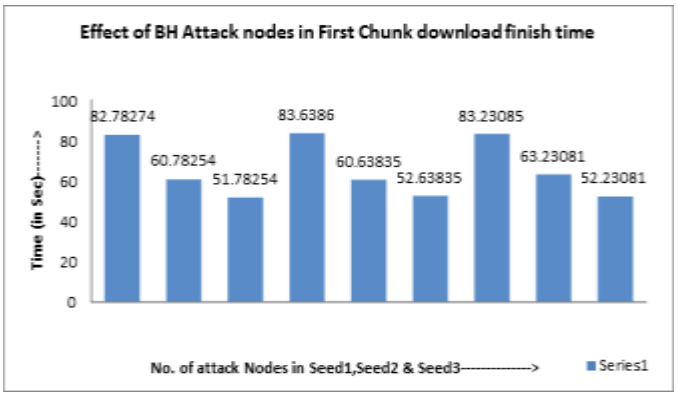

Figure 2: Effect of BH Attack nodes in First Chunk download finish time

Figure 2 represents Effect of black hole Attack nodes in First Chunk download finish time. Here the number of attack nodes are 1,2 and 3 for seeds 1,2 and 3 for swarm size of 10. Here we observe that, because of black hole attack the first chunk download time has increased drastically.this means because of Black Hole attack the service start time won't be affected but after sometime it will start affecting the whole video on demand service because the attacking notes are drastically accepting the first sem download finished and because of which the service will be delayed. The effect of Black Hole attack nodes on Swarm of different sizes are almost similar, thatis, the number of attack nodes increases the total download finish time for the first chunk hunk for the first chunk increases drastically.The increased number of attack notes causes more damage to the first chunk download finish time

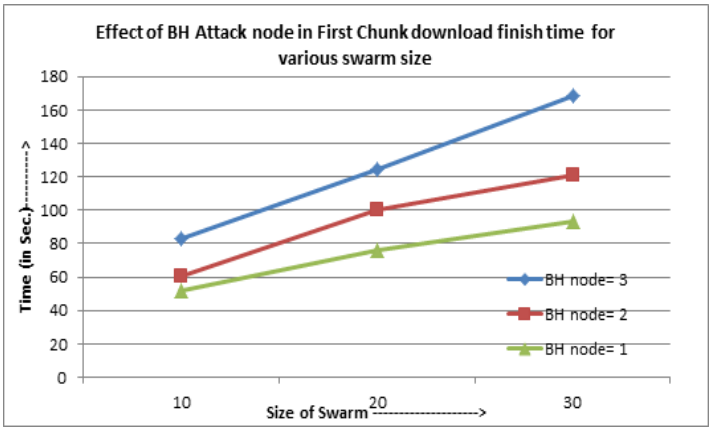

Figure 3:Effect of BH Attack node in First Chunk download finish time for various swarm size

Figure 3 represent comparative study of effect of black hole attack on various sizes of swarm. Here number of black hole attack nodes are 1,2 and 3 for swarm size of 10 , 20 and 30. Here we have found that as the number of attack nodes increases the percentage increase in first chunk download time is around 25% to 30 %.

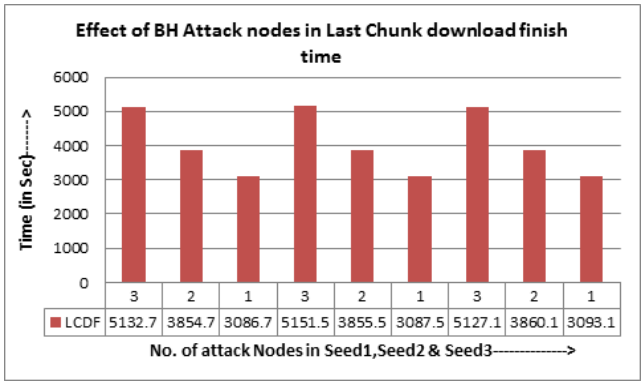

Figure 4 Effect of BH Attack nodes in Last Chunk download finish time

Figure 4 represents the Effect of BH Attack nodes in Last Chunk download finish time. the last jump download finish time is an important parameter for measuring the performance of Video on demand services it is because if the last song download finish time takes more time the overall performance of the system will be deteriorated the effect of Black Hole notes here are severe as the number of attacking notes increases the time required to download the last chance also increases.Here the observation was taken for various numbers of seeds.

Figure 5 represents Effect of BH Attack node in Last Chunk download finish time for various swarm sizes.

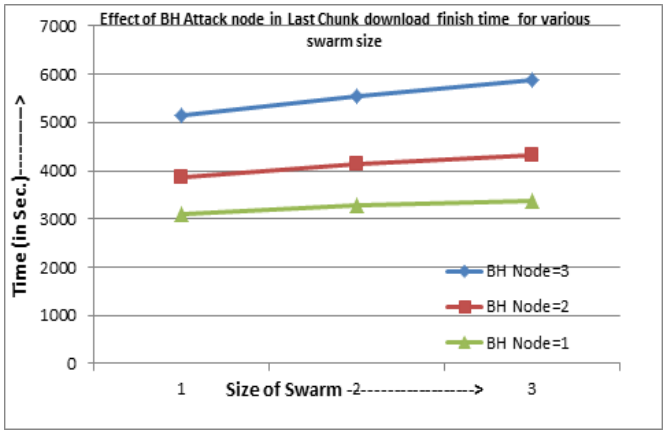

Figure 5: Effect of BH Attack node in Last Chunk download finish time for various swarm size

The table 1 below represents the average throughput that we have obtained from various simulations of Black Hole attack in different from sizes of p2p based Video on demand services

TABLE 1: AVERAGE THROUGHPUT

No. of BH Node	Size of swarm	Seed 1	Seed 2	Seed 3
0(No Attack)	*10*	*8582*	*8574*	*8951*
1	10	5711	5742	5704
2	10	4291	4293	4293
3	10	3442	3432	3444
0(No Attack)	*20*	*8951*	*8911*	*8821*
1	20	5851	5831	5821
2	20	4371	4341	4341
3	20	3481	3481	3489
0(No Attack)	*30*	*9741*	*9751*	*9851*
1	30	6241	6201	6111
2	30	4531	4521	4501
3	30	3521	3501	3511

The above table represents average throughput for simulations with 0, 1,2 and 3 black hole attack node for swarm size 10, 20 and 30 for seed 1,2 and 3

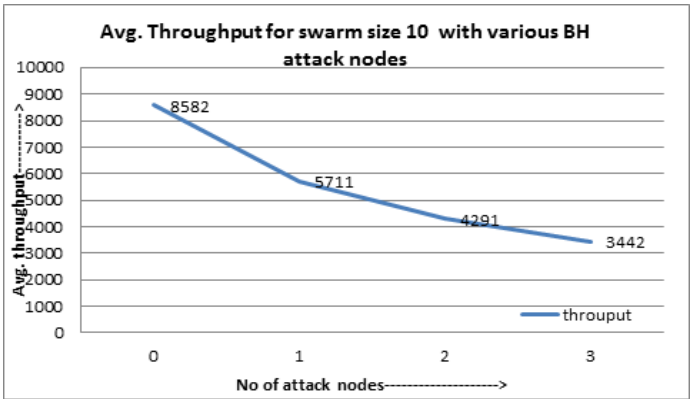

Figure 6 Avg. Throughput for swarm size 10 with various black hole attack nodes

Figure 6 represents a pictorial representation of average throughput for swarm size of 10.we had not represented the same graph for different sizes of Swarm intentionally due to space constraints and its repetitive nature.Initially, when there was no attack the throughput was much the throughput was much higher but when there was a single attacking node, the average throughput decreased drastically and also decreased for anincreased number of attacking nodes

VI. CONCLUSION

From the above mentioned that we can conclude that the black hole attack on p2p based Video on demand services are severe However, the number of attacking notes doesn't affect the starting connection time, but it does affect overall performance. Relatively the effect of Black Hole nodes is lesseffective in small swarm sizes.But it is prominent in larger swarm sizes.It is because large size network generally hasa large number of communications among themselves. Hence, it gives attackers more opportunity for performing attack. So, for the purpose of sharing some important file, limited swarm will be less prone to any sort of black hole attacks.

REFERENCES:

[1] 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 Surveys & Tutorials, vol. 7, no. 2, pp. 72- 93, 2005.

[2] Majumder, Sudipta & Hussain, Anwar. (2011). Attack Patterns for Black Hole, Gray Hole and Worm Hole Attack on Adhoc Networks. International Journal of Mobile &Adhoc Network.

[3] R. Wang, Y. Shoshitaishvili, C. Kruegel, G. Vigna, "Steal This Movie: Automatically Bypassing DRM Protection in Streaming Media Services", *Proceedings of the 22nd USENIX Security Symposium*, 2013.

[4] V. Piccioli, "E-Learning Market Trends & Forecast 2014-2016 Report", *Tech. Rep.*, 2014
[5] N. Liogkas, R. Nelson, E. Kohler, and L. Zhang, "Exploiting BitTorrent for fun (but not profit)," In IPTPS'06, 2006
[6] M. Piatek, T. Isdal, T. Anderson, A. Krishnamurthy, and A. Venkataramani, "Do incentives build robustness in BitTorrent" Proc. Of the 4th USENIX Symposium on Networked Systems Design & Implementation, pp. 1-14, 2007
[7] P. Dhungel, D. Wu, B. Schonhorst, and K. W. Ross, "A measurement study of attacks on BitTorrent leechers," in IPTPS'08, pp. 7-7, 2008