Effects of Grey-Hole Attack onP2P Based Video on Demand (VoD) Services

Sudipta Majumder [#1], Md. Anwar Hussain [*2]
[#1]Dept. of CSE, DUIET, Dibrugarh University,Assam, India.
[*2]Dept. of ECE, NERIST, Arunachal Pradesh, India.

Abstract--*Peer to peer networks are venerable to various types of attacks. These attacks degrade the performance of the P2P based network.in this paper, we have presented the effect of Grey-hole attack especially in the case of BitTorrent based VoD services .we have simulatedGrey-hole attacks and studied the effect of anumber of malicious nodes in apeer 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 thetotal 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--*Grey 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

Peer-to-Peer (P2P) systems are set of thesystem which is distributed systems. They may or may not have a minimal centralized control or hierarchical organization depending upon the type of architecture of the system.In peer to peer system, all the nodesare symmetric in term of functionality. Since P2P systems are distributed in nature, so they perform thecritical function as thedistributed system performs. Hence P2Psystem performs resources localization like vital tasks in a decentralized manner. Like manyother networking systems, P2P systems have a large number of challenges and those challenges consistof designing and implementation a robust distributed system composed of distributed and heterogeneous peer nodes, located in unrelated administrative domains.

Peer networks have a very large share in terms network traffic. Still, the concept of peer to peer network is a bit controversial. The reason for being controversial is that many experts claim there is nothing much new in peer to peer network. In fact, there are many definitions available for peer networks. As defined in [1], "P2P allows file sharing or computer resources and services by direct exchange between Systemsor"allows the use of devices on the Internet periphery in a non-client capacity".Also, "it could be defined through three key requirements:

a) They have an operational computer of server quality,

b) They have a DNS independent addressingsystem and

c) They are able to scope with variable connectivity.

Also, as defined in [2]: "P2P is a class of applications that takes advantage of resources-storage, cycle, content, human presence-availability at the edges of theInternet. Because accessing to these decentralized resources means operating in anenvironment with unstable connectivity and unpredictable IP addresses." P2P nodes must operate outside the DNS system and have significant or total autonomy from central servers [1].

II. PEER NETWORK ATTACK TYPES

There have been many types of attacks in peer to peer networks. The main motive behind the attacks is to disrupt the network or to gain unsolicited access to the content etc. There are various types of attacks on the P2P network. And they can be categorized into two categories which are active attack and passive attack. The attacks which mainly target the nodes and try to damage the nodes can be referred as anactive attack.The resource exhaustion attack, opportunistic attack, worm infection, zombification attack, eclipse attack etc. are the example of active attack[3][4][5][6]. Whereas the second class of attacks, passive attack, is defined as the attacks which try to disrupt or damage the P2P network itself. They do the attack in order to restrict the peer's access to the network.Cached data attack, Sybil attack, bootstrapping attack etc. are the example of apassive attack.[7][8][9].

III. GREY HOLE ATTACK

One of the prominent passive attacks on peer to peer network is grey hole attack. In this type of attack, there are some malicious nodes which act as grey hole nodes. These nodes facilitate the execution of the attack on the network. The attacking nodes act as a normal node in the beginning of the communication in the peer to peer network. But after some time their malicious behavior gets activated by some triggering.

These attackers mainly affect the underlying network of the P2P network**.**

The attacking node first publishes a false torrent file of a rare file to the internet. Then some user tries to communicate with the attacking node in search of a file in demand.In thedue course of transfer of a.torrent file, the attacking nodes get the IP address of the user. Now within alimited time, the attacking node publishes a false routing table of the network declaring that a certain peer which have the file in demand to be his neighbor. Now when the user sends a request, it re-routes the communication through it. Thus causing adelay in the network. Now, when the communication has started, after sometime, it intentionally drops acertain key chunk of the data/file. [10]

IV. GREY-HOLE ATTACK SIMULATION AND RESULT ANALYSIS

Gray hole attack is an active attack type, which leads to dropping of messages. Attacking node first agrees to forward packets and then fails to do so. Initially, the node behaves correctly and lays true RREP messages to nodes that initiate RREQ message. Afterwards, the node just drops the packets to launch a (DoS) denial of service attack. If neighboring nodes that try to send packets over attacking nodes lose the connection to thedestination they may want to discover a route again, broadcasting RREQ messages. Attacking node establishes a route, sending RREP messages. This process goes on until malicious node succeeds in its purpose.

In the fig.1, we have observed that the Grey-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.

Fig.2 represents Effect of grey-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 Grey-hole attack the first chunk download time has increased.

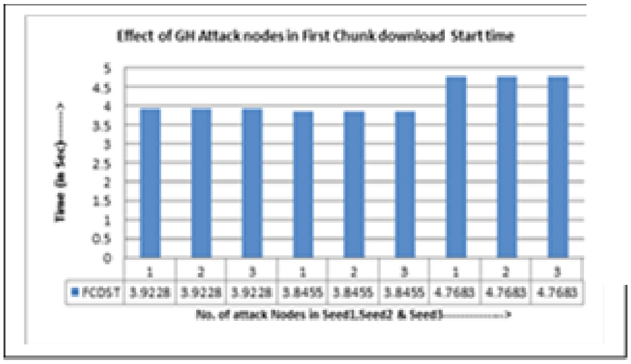

Fig.1: Effect of GH Attack nodes in First Chunk download Start time

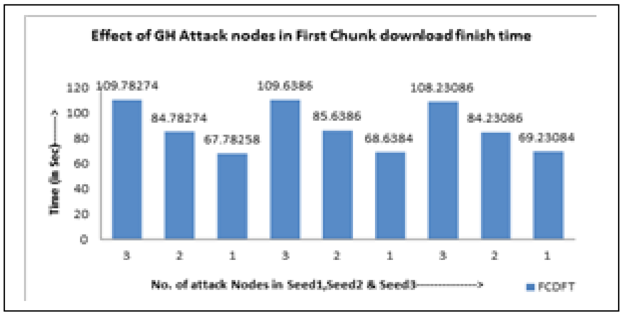

Fig.2:Effect of GH Attack nodes in First Chunk download finish time

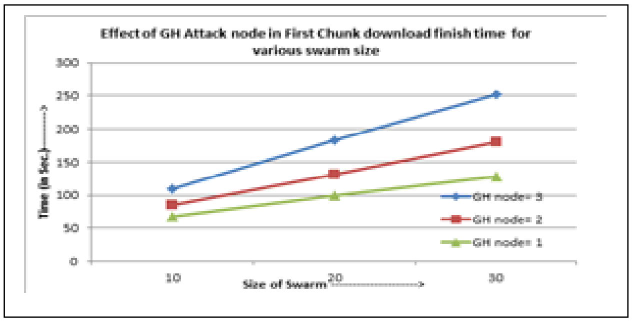

Fig. 3:Effect of GH Attack node in First Chunk download finish time for various swarm size

Fig.3 represent thecomparative study of theeffect of grey hole attack on various sizes of theswarm. Here anumber of grey hole attack nodes are 1,2 and 3 for swarm size of 10, 20 and 30.Fig.4 represents the Effect of grey hole Attack nodes in Last Chunk download finish time. Here the observation was taken for various numbers of seeds.

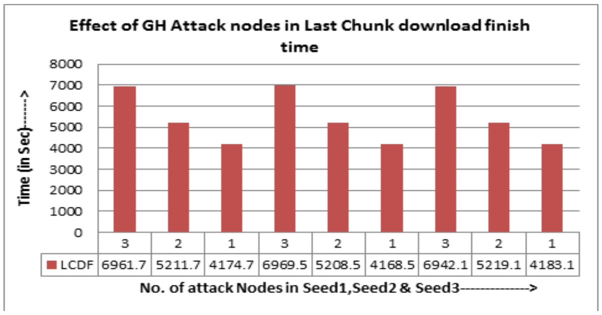

Fig.4:Effect of GH Attack nodes in Last Chunk download finish time

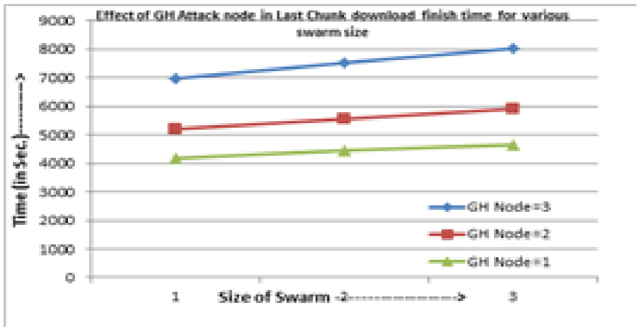

Fig. 5:Effect of GH Attack node in Last Chunk download finish time for various swarm size

The table 1 below represents the average throughput that we have obtained from various simulations of Grey Hole attacksin adifferently sized swarm of p2p based Video on demand services.

TABLE 1: AVERAGE THROUGHPUT FOR GREY HOLE ATTACK SCENARIOS.

No. of Grey Hole Node	Size of swarm	Seed 1	Seed 2	Seed 3
0(No Attack)	*10*	*8582*	*8574*	*8951*
1	10	7751	5802	7734
2	10	5801	5801	5814
3	10	4651	4642	4664
0(No Attack)	*20*	*8951*	*8911*	*8821*
1	20	8001	7851	7831
2	20	5881	5911	5901
3	20	4691	4721	4701
0(No Attack)	*30*	*9741*	*9751*	*9851*
1	30	8591	8631	8451
2	30	6241	6341	6061
3	30	4881	4761	4631

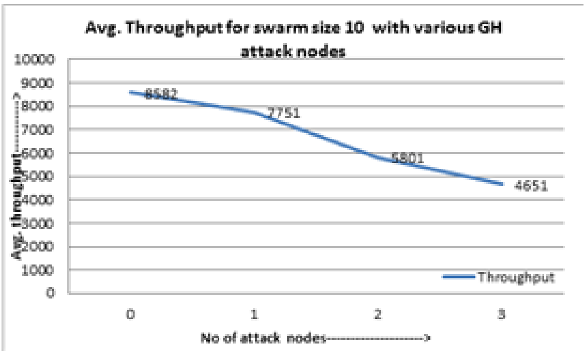

Fig. 6: Avg. Throughput for swarm size 10 with various GH attack nodes

Figure 6 represents a pictorial representation of average throughput for swarm size of 10 for grey hole attacks. 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 higher but when there was a single attacking node, the average throughput decreased drastically and, it also decreasedby an increased number of attacking nodes

V. CONCLUSION

From the above mentioned discussion, that we can conclude that the grey 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 Grey Hole nodes is less effective in small swarm sizes. But it is prominent in larger swarm sizes. It is because large size network generally has a large number of communications among themselves. Hence, it gives attackers more opportunity for performing theattack. So, for the purpose of sharing some important file, thelimited swarm will be less prone to any sort of Grey hole attacks.It is important to mention that number of seeders have inverse effect on grey hole attacks.

REFERENCES:

[1] Peer-to-Peer Working Group, Bidirectional Peer-to-Peer communication with interposing Firewalls and NATs, White Paper, 2001.

[2] R. Steinmetz and K. Wehrle, peer to peer Systems and applications, (Eds) Springer LNCS 3485, 2006.

[3] Kannan, Jayanthkumar,and LakshmiNarayanan, Karthik, “Implications of Peer-to-Peer Networks on Worm Attacks and Defenses”, CS294-4 Project,Fall 2003, For Computer Science Dept. of Berkley University.

[4] Castro, M., Druschel, P, Ganesh, A., Rowstron, A. and Wallach, D.S., “Secure routing for structured peer-to-peer overlaynetworks", In Proceedings of USENIX Operating System Design and Implementation (OSDI), Boston, MA, Dec. 2002.

[5] Engle, Marling, “Vulnerabilities of P2P Systems and a Critical look at Their Solutions”, April 2006.

[6] Yu, Wei, Boyer, Corey, Chellappan, Sriram and Xuan, Dong, “Peer-to-Peer System-based Active Worm Attacks: Modeling and Analysis”, In Proc. of IEEE International Conference on Communications (ICC), pp. 295-300, May 2005.

[7] Yolum, Pinar, Singh and Munindar P., “Flexible Caching in Peer-to-Peer Information Systems”, In Proceedings of the 4th International Bi-Conference Workshop on Agent-Oriented Information Systems (AOIS), Bologna, July 2002.

[8] Stading, Tyron, Maniatis, Petros and Baker, Mary, “Peer-to-Peer Caching Schemes to Address Flash Crowds (2002)”, In1stInternational Peer To Peer Systems Workshop (IPTPS 2002).

[9] Douceur, John R., “The Sybil Attack”, In Proceedings for the 1st International Workshop on Peer-to-Peer Systems (IPTPS ’02), Cambridge, Massachusetts, USA, March. 2002.

[10] S.Majumder, A.Hussain, "how to increase per-session throughput in distress hours if grey hole attack is in-avertible”, ISSN(online): 2277- 128X, IJARCSSE, Volume 4, Issue 11, November 2014.