AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

Modeling the Performance of DDoS Attack in Optical Burst Switched Networks

[1]A.M. Balamurugan and [2]A. Sivasubramanian

[1]*Associate professor, St. Joseph's college of Engineering, Chennai-600119, TamilNadu, India.*
[2]*Principal, Tagore Institute of Engineering and Technology, Deviyakurichi, Aathur Taluk, Salem-636112, Tamil Nadu, India.*

ARTICLE INFO

Article history:
Received 19 August 2014
Received in revised form
19 September 2014
Accepted 29 November 2014
Available online 15 December 2014

Keywords:
Optical Burst switching, Distributed denial of service attack, Header rejection, Survivability

ABSTRACT

The Optical Burst Switching (OBS) is an evolving result to the technology concern that could achieve a viable network in future. They are endowed with the capacity to meet the bandwidth constraint of those applications that require intensive bandwidth. The field of optical transmission has undergone numerous advancements and is still being researched mainly due to the fact that optical data transmission can be done at enormous speeds. The concept of switching in networks has matured enormously with several researches. Adaptive Optical burst switching is regarded as feasible solution for switching bursts over networks but has several drawbacks. However we have elucidated the attacks concerned with OBS and with respect to the distributed denial of service (DDoS) attack. The various header rejection probability was determined among one of the several models in the queuing theory. It has be inferred that a drastic reduction in header rejection probability occurs by increasing the size of the active flows in the OBS network.

To Cite This Article: A.M. Balamurugan and A. Sivasubramanian, Modeling the Performance of DDoS Attack in Optical Burst Switched Networks. ***Aust. J. Basic & Appl. Sci.,*** *8(18): 479-482, 2014*

INTRODUCTION

Optical Internet has grown to be the main channel for all types of virtually chipping in communications around the world due to the exceptional growth in traffic volumes. The number of users and the diversity of applications demand more and more bandwidth that keeps increasing day by day. These ever-increasing demands need ever-increasing bandwidth. (Chlamtac. I, Ganz. A, Karmi. G, 1992). Here optical communication comes into the picture. It provides a huge amount of bandwidth and leads to the popular concept of optical Internet. A broad range of experimental switching technologies are presented to support Internet Protocol (IP) over wavelength-division multiplexing (WDM) in optical telecommunications networks. The concept of optical burst switching (OBS) refers to a group of such switching technologies. Unlike optical packet switching, it does not require optical buffering. It combines the recompenses optical packet switching and circuit switching. It is regarded as a viable solution for transmitting bursts over an optical network. (Qiao. C, Yoo. M. 1999). A connection is setup uniquely for the transmission of a single burst. An OBS network consists of OBS nodes interconnected with WDM fiber in a mesh topology. The OBS architecture is shown in figure 1.

There are lots of potential threats present in the OBS networks. In order to have secure and better communication, the data burst should follow the control signal path from source to destination node. It should be processed by each node in the network link. The node tries to duplicate or steal information from the control signals because control signals are processed by all intermediate nodes in the network. (A.M.Balamurugan, Dr.A.Sivasubramanian 2013). The identified threats are *Orphan Bursts, Redirection of Data Bursts, Replay, Burst header flooding attacks, Fake burst header attack and Denial of service attack.* (Sreenath. N, Muthuraj. K, Vinoth. G.2012) Out the various types of attacks, this work looks into the DDoS flooding attack alone in particular. Though many studies have been carried about these attacks. Hence our network should be made secure. The various principles of providing this security are Burst confidentiality at Ingress and Egress routers, Per Hop Header authentication, and Burst integrity. (Fok, M.P, Zhexing Wang , Yanhua Deng , Prucnal, P.R.2011) (A. M. Balamurugan and A. Sivasubramanian.2014)

The rest of the paper is organized as follows. Section 2 gives the overview of DDoS attack and queuing models to analyze the header rejection probability. Section 3 will give the results and discussions of our work.

Corresponding Author: A.M. Balamurugan, Research Scholar and Associcate Professor, St. Joseph's College of Engineering, Chennai-600119, Tamilnadu, India.
E-mail: bala_am2000@yahoo.com

Australian Journal of Basic and Applied Sciences, 8(18) December 2014, Pages: 479-482

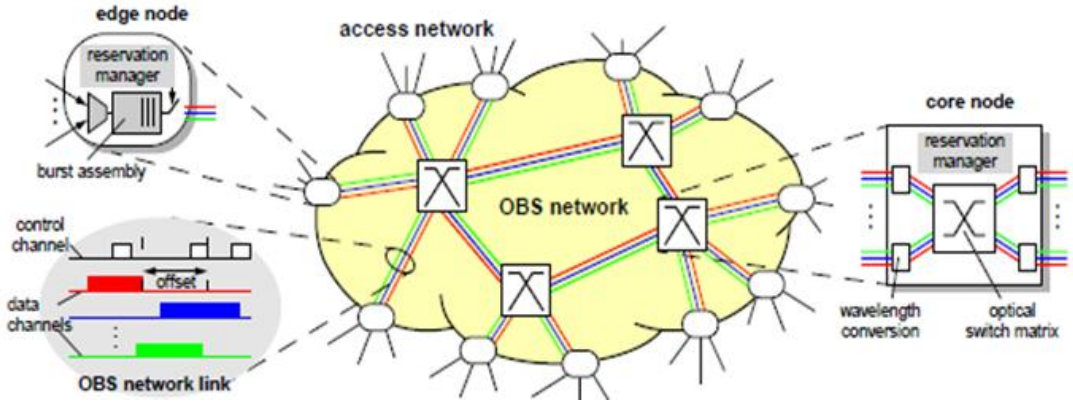

Fig. 1: OBS architecture.

Ddos flooding attack:

A DDoS flooding attack is an attack that attempts to make a failure in a network by giving more inputs than the network nodes can process properly (Yuhua Chen, Pramode K. Verma and Subhash Kak. 2009). OBS core routers make scheduling decisions based on the availability of their outgoing WDM channels. When a burst is scheduled, the core router will mark the WDM channel 'busy' for the duration of the burst. In the case where no 'idle' WDM channel can be found for the upcoming burst, the burst is discarded. Note that all scheduling decisions are made by processing burst information carried in burst headers on-the-fly. The OBS core routers have no ability to verify if indeed the scheduled optical burst arrived at the designated time. This can be used to launch a denial-of-service attack by simply injecting malicious burst headers, causing the core routers to mark WDM channels 'busy' and thus blocking real traffic passing through the OBS network.

It seems the case of legal packets reassignment is the most serious problem. In this paper, we modeled the DDoS attack with the help of queuing theory. We are assuming that the header flow generation rate satisfies the Poisson distribution. So the attacker node can be modeled by Poisson distribution. The header treatments differ from time to time. Depending the availability of wavelengths, the header admission and rejection takes place. If the incoming channel is free, the burst header will be processed by the core router or else it will simply discarded. So it takes a random time. Here we assume the header service time satisfies the exponential distribution. It is a wide used assumption in telecommunication models

Let us make the following designation

λ – headers generating rate;
μ – header service rate;
δ – number of nodes involved to the flooding attack
N – the buffer size for headers.

It is offered to describe the headers buffer behaviour by M/M/1/N+1 queuing system. The designation M/M/1/N+1 reflects traditional queuing theory nomenclatures, whereby

1.The first M defines the cumulative distribution function of inter-arrivals times of burst headers. The arrival process is considered as Poisson process.
2. The second M describes the burst header service time probability.
3. In both cases, random inter-arrival times and random service times are supposed to be independent.
4. The third term gives the meaning any core node can treat only one burst header at a time.
5. The next item means, that the maximum number of headers in the OBS node buffer is N.
6. An arriving header enters the buffer if it finds fewer then N headers in the buffer and is lost Otherwise.

Let P_k be the probability of k burst headers in the queue of AOBS core node. Therefore, the steady-state probabilities for AOBS node buffer under the flooding attack are as follows

$$P_K = \frac{\left((1-\rho)\rho^K\right)}{\left(1-\rho^{K+1}\right)} \quad (1)$$

$$\text{Here } \rho = \frac{\lambda\delta}{\mu} \quad (2)$$

The headers rejection probability is defined as

$$P = \frac{\left((1-\rho)\rho^N\right)}{\left(1-\rho^{N+1}\right)} \quad (3)$$

In similar manner the survivability of header is calculated as

$$Q = 1 - \frac{\left((1-\rho)\rho^{N}\right)}{\left(1-\rho^{N+1}\right)} \quad (4)$$

The next section will give the performance comparison of Header blocking probability with the number of attacker node differs.

RESULTS AND DISCUSSIONS

Our Simulation scenario is depicted in figure 2. For our simulation we consider three client networks connected to an OBS Ingress node via 1Gbps link. The Ingress nodes are connected via core nodes with the link capacity of 20Gbps.The client network will generates the packets with the size of 1500 bytes/packet. The Ingress node will aggregate these packets into Burst. The Burst size will vary from 40000 packets/burst to 1, 20,000 packets burst.

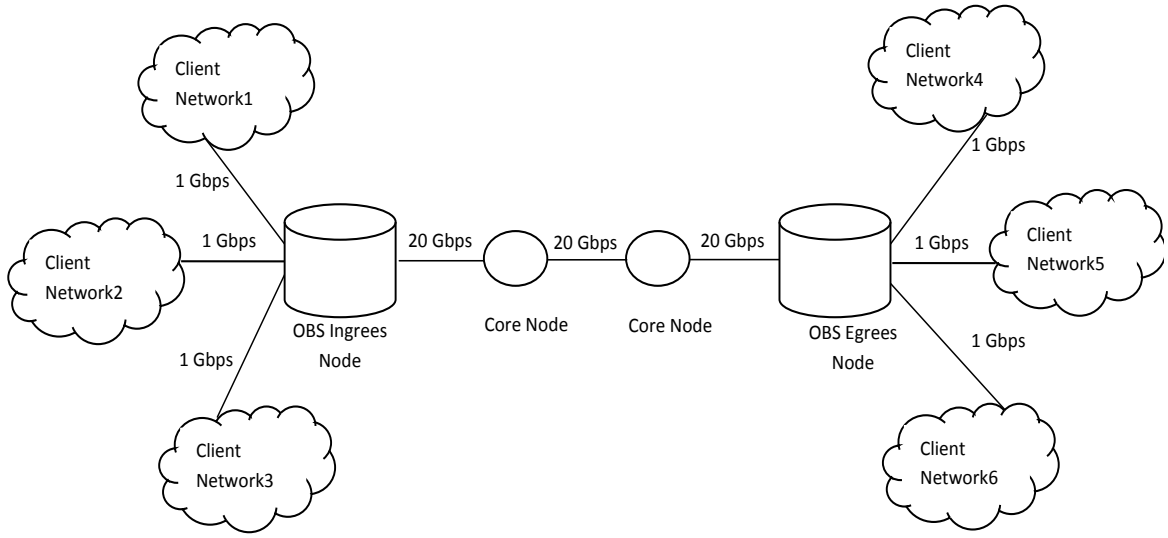

Fig. 2: Simulation Scenario

From this simulation we are trying to find out the performance of burst transmission in the case of DDoS attacks. The header rejection and survivability rates are calculated for an increase attacker nodes using Queuing model what has been discussed in the section 2.The average time taken for a burst (40000 packets) to reach the ingress node via 1Gbps link is 0.48seconds. The arrival rate of the burst header is calculated for every 60 seconds. The minimum burst header processing time at the core node is assumed to 0.1 seconds. The service rate of the burst header is sum of arrival rate and header processing time at the number of intermediate core routers.

Table 1: Header Rejection Probability.

Burst size (packets/ Burst)	*Arrival rate/sec*	*Service rate/sec*	*Number of Attacker nodes*		
			n=1	*n=2*	*n=3*
40000	*125*	*88*	*0.45*	*0.67*	*0.77*
50000	*100*	*75*	*0.43*	*0.65*	*0.76*
60000	*83*	*65*	*0.41*	*0.64*	*0.75*
70000	*71*	*58*	*0.40*	*0.63*	*0.74*
80000	*63*	*52*	*0.39*	*0.63*	*0.74*
90000	*56*	*47*	*0.39*	*0.62*	*0.73*
100000	*50*	*43*	*0.38*	*0.61*	*0.73*
110000	*45*	*40*	*0.37*	*0.60*	*0.72*
120000	*42*	*37*	*0.37*	*0.61*	*0.72*

From the Table 1 we can conclude that the effect of burst rejection has increased due to the increase in the number of attacker nodes. But one key interesting point from this observation is that, when the burst size increases from 40000 packets to 120000 packets the header rejection probability slightly reduces from 0.45 to 0.37 in the case of one attacker node. It is observed that when the burst size reduces a certain level, a drastic reduction in the burst header rejection probability occurs in the case of higher attacker nodes in the network. In order to increase the burst size to the expected level we can increase the number of active flows in the OBS network.

Australian Journal of Basic and Applied Sciences, 8(18) December 2014, Pages: 479-482

Conclusion:

Therefore it can be concluded that Adaptive Optical Burst Switching (AOBS) is not only cost effective but also a promising area of research in the near future. The properties of secure communication and the attacker node behavior in AOBS network have been explicated. Furthermore the several attacks and vulnerabilities that affect the bursts are also discussed. We have also simulated and studied the header rejection and survivability probabilities under different strength of attacking nodes. The results indicate that if the size of the active flows increases in the AOBS, the header rejection probability will drastically reduce. But it cannot be completely prevented. The right solution would be to provide Burst confidentiality at Ingress and Egress routers, Per Hop Header authentication, and Burst integrity.

REFERENCES

Balamurugan, A.M. and A. Sivasubramanian, 2014. "Quantum Key Based Burst Confidentiality in Optical Burst Switched Networks," The Scientific World Journal, vol. 2014, Article ID 786493, 7 pages, doi:10.1155/2014/786493

Balamurugan, A.M., Dr. A. Sivasubramanian, 2013. Optical burst switching issues and its features, International journal of Emerging Trends & Technology in computer science, 2(3): 306-315.

Chlamtac, I., A. Ganz, G. Karmi, 1992. Lightpath communications: An approach to high bandwidth optical WAN's, Communications,IEEE Transactions, pp: 1171 -1182.

Fok, M.P., Zhexing Wang, Yanhua Deng, P.R. Prucnal, 2011. Optical Layer Security in Fiber-Optic Networks, Information Forensics and Security, IEEE Transactions on, 6(3): 725–736.

Qiao, C., M. Yoo, 1999. Optical burst switching (OBS) : A new paradigm for an optical internet. Journal of High Speed Networks, (8): 69-84.

Sreenath, N., K. Muthuraj, G. Vinoth, 2012. Threats and Vulnerabilities on TCP/OBS networks, Computer Communication and Informatics (ICCCI), International Conference, pp: 1–5.

Yuhua Chen, K. Pramode Verma and Subhash Kak, 2009. Embedded security framework for integrated classical and quantum cryptography services in optical burst switching networks, Security and Communication Networks.