International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-2 Number-1 Issue-3 March-2012

Identification of current attacks and their counter measures in Optical Burst Switched (OBS) network

Siddharth Singh Chouhan[1], Sanjay Sharma[2]
Department of Computer Science & Engineering OIST Bhopal, India[1,2]

Abstract

As day by day application grows internet requires large amount of bandwidth. Optical Burst Switching (OBS) is the next generation optical Internet with IP over WDM as the core architecture. It can achieve a balance between Optical Circuit Switching (OCS) and Optical Packet Switching (OPS). Optical network supports huge bandwidth and transmits data at an average rate of 50Tb/s. But we need to exploit the fiber's huge bandwidth through WDM which is the current favorite multiplexing technology in Optical communication networks. OBS is a trusted mechanism used for optical switching. Optical burst switching has been positioned as a viable means of implementing optical communication efficiently. This review paper identifies potential threats to security in OBS networks. Solutions in each category are examined, and research directions are presented.

Keywords

Optical communication, Optical burst switching, Optical packet switching, Optical circuit switching.

1. Introduction

The tremendous growth of the Internet and the World Wide Web, both in terms of number of users and the amount of time, and thus bandwidth taken by each user, is a major factor. Internet traffic has been growing rapidly for many years. Estimates of growth have varied considerably over the years, with some early growth estimates showing a doubling every four to six months. Despite the variations, these growth estimates are always high, with more recent estimates at about 50% annually. Fiber to the home has shown steady growth with Asian markets showing the highest market penetration.

At the same time, businesses today rely on high-speed networks to conduct their businesses. There is also a strong correlation between the increase in demand and the cost of bandwidth [3].

1.1 Optical network communication

It is the technology which full fill the requirement. These networks are also increasingly becoming capable of delivering bandwidth in a flexible manner where and when needed. An optical network provides a common infrastructure over which a variety of services can be delivered. Optical communication is any form of telecommunication that uses light as the transmission medium [2].It is the preferred medium for transmission of data at anything more than a few tens of megabits per second over any distance more than a kilometer. It is also the preferred means of realizing short-distance high-speed interconnections inside large systems.

The amount of deployment of fiber is often measured in sheath miles. Sheath mile's is the total length of fiber cables, where each route in a network comprises many fiber cables .An optical network less susceptible to various kinds of electromagnetic interference and other undesirable effects. When we talk about optical networks, we are really talking about two generations of optical networks. In the first generation, optics was essentially used for transmission and simply to provide capacity. Second-generation optical networks have routing, switching, and intelligence in the optical layer. Optical fiber offers much higher bandwidth than copper cables.

Multiplexing that provides the capacity needed to realize these networks. Time Division Multiplexing (TDM) is a method of putting multiple data streams in a single signal by separating the signal into many segments, each having a very short duration. Each individual data stream is reassembled at the receiving end based on the timing. Wavelength Division Multiplexing is essentially the same as frequency division multiplexing (FDM), which has been used in radio systems for more than a century. For some reason, the term FDM is used widely in radio communication, but Wavelength Division Multiplexing (WDM) is used in the context of optical communication is a technology which multiplexes a number of optical carrier signals onto a single optical fiber by using different wavelengths (i.e. colors) of laser light. WDM thus provides virtual fibers, in that it makes a single fiber look like multiple "virtual" fibers, with each virtual fiber carrying a single data stream.

1.2 Optical burst switching

OBS is the next generation optical Internet with IP over WDM as the core architecture. It is an emerging solution to achieve all-optical WDM Networks. It can achieve a balance between OCS and OPS. OBS requires limited delay of the data at intermediate nodes as in OCS, and ensures efficient bandwidth utilization on a fiber link just as in OPS [6 7]. One of the main aspects in the deployment of OBS services is the development of an optical traffic/performance monitoring scheme allowing the provision of user-specified quality of service (QoS). An alternative approach called OBS, which combines the best of optical circuit switching and optical packet switching, was proposed in as a future high-speed switching technology and has received an increasing amount of attention from both academia and industry worldwide [1].

OCS is relatively easy to implement but lacks the flexibility to cope with the fluctuating traffic and the changing link status. A circuit-switched network provides circuit-switched connections to its customers. In circuit switching, a guaranteed amount of bandwidth is allocated to each connection and is available to the connection all the time, once the connection is setup. The sum of the bandwidth of all the circuits, or connections, on a link must be less than the link bandwidth. The most common example of a circuit switched network is the Public-Switched Telephone Network (PSTN).

In OBS network multiple IP packets with the same destination are assembled into a burst at an ingress OBS node and the burst is transmit through the network core entirely in the optical domain [2 4].OPS is conceptually ideal, but the required optical technologies such as optical buffer and optical logic are too immature for it to happen anytime soon. Packet switching features delivery of variable-bit-rate data streams (sequences of packets) over a shared network. When traversing network adapters, switches, routers and other network nodes, packets are buffered and queued, resulting in variable delay and throughput depending on the traffic load in the network. Packet switching is a digital networking communications method that groups all transmitted data regardless of content, type, or structure into suitably sized blocks, called packets.

The area of security in Optical networks is very important to manage. In addition, the issues related to physical network security has been deal with respect to Optical networks. Optical burst switching technology has the potential to be deployed today on a commercial scale to speed up the provisioning of end-to-end optical paths between and among communicating entities. Because of the unique characteristics of OBS networks, there is a degree of security vulnerability associated with the burst. Proposed work is intend to find the possible security threats that may happen in Optical Burst Switched Networks and the counter measures are examined separately. Upon a network can be broadly categorized into many areas based on the goal of the attacker some are: Traffic analysis, Eavesdropping, Data delay, Service denial, QoS degradation, Spoofing, and Burst Duplication Attack [8].

There are many other possible ways to divide the attack taxonomy problem. For instance, each attack can be categorized by its resources (passive, active); its means of attack (transmission/reception, protocol, control system); the target (specific users or network/sub network); the intended effect (traffic analysis or eavesdropping or service disruption); the location of the attack (terminal, node, link, multiple locations), and the attacker's willingness to be discovered (covert, subtle, overt).The main resulting attack types are reduced to two: eavesdropping & traffic analysis ('eavesdropping'), and service disruption [8].

2. Literature Review

In 2011, Marija Furdek [1] proposed the idea of prevention oriented network planning in WDM optical network communication network planning approaches which deal with the physical-layer security issues in transparent optical networks and emphasizes the need for new, preventive strategies for increasing safety in transparent optical networks. The author in the paper points out some of the common network planning and design. Than describes about the different types of attacks in transparent optical networks, by an overview of specific attack methods which exploit optical network component vulnerabilities followed with the identification of key issues in fault and attack management in transparent optical networks.

In 2010, Md. Shamim Reza, Md. Maruf Hossain and Satya Prasad Majumder [2] proposed work is to minimize burst loss rate in the network**.** Discussed about the performance of an optical burst switching network. The performance measure in terms of burst loss rate is evaluated and wavelength converters have been used for contention resolution when two or more bursts contend for the same wavelength at the same output port. They found that performance improves for greater number of wavelength

converters and network wavelengths. They have also seen if the network design parameter is constant then loss increases as the traffic or burst arrival increases.

In 2011, P. Siva Subramanian and K. Muthuraj proposed work is intended to find the possible security threats that may happen in Optical Burst Switched Networks and provide their counter measures. In the paper the identified burst duplication attack in which intermediate core router to create a duplicate copy of the control burst and modify its value to create a path between the attacker and the compromised node. In such a case, the data burst which will be coming transparently after an offset time will be sent to the original destination as well as to the attacker. Thus attacker compromises the integrity of the data burst. The suggested countermeasures to detect and remove the attack first method makes use of digital signature and the second method trusted node is used to detect and remove the attack.

In 1998, Medard et.al [8] proposed a new method for detecting attacks. In the work they have first considered advantages and limitations of both classes of methods that is applications of existing methods used in traditional networks and the new method for detecting attacks in optical network communication. The new detection scheme presented provides some defenses against sporadic jamming and some defenses against multipoint attacks assuming an advance algorithm running in a network management system.

2.1 Examination of Threats

Several threats have been identified from the previous work and examine them and accordingly the all have been tabularized in Table 1.

2.2 Threats Classification

On the basis of different issues threats have been classified and presented in the tabular form.

Table 1: Comparison of Threats

Threats	Class	Cause	Remedy
Traffic analysis [1]	Intended effect	It extracts the information which is been communicated between the sources in a secure way.	Power detection methods/Masking etc.
Eavesdropping [1]	Intended effect	It is similar in properties with traffic analysis but differ at the level of the layer when it is applied whether on the physical layer or on the higher layers.	Power detection methods /Optical Spectral Analysis Methods/Mutual authentication.
Spoofing [1]	Active/Passive attack	It is the type of attack which is attempting to gain access to a system by using a false identity than after elevation of privileges or abuse using authorization can begin.	Cryptographic methods
Burst Duplication Attack [5 6]	Active/Passive attack	Intermediate core router duplicates a control burst and modifies its value to create a path between itself and attacker	Digital signature/ Trusted node method
Service disruption [1]	Intended effect	It is a type of attack which prevents communication or Degrades the quality of service (QoS).	Prevention oriented Network planning.
Physical-layer attacks (Direct attacks, Indirect attacks, Pseudo-attacks)	Intended effect	Causes jamming ,local or remote attacks, crosstalk, Unauthorized access through add/drop ports, anomalies which are not intrusions, but may be interpreted as such, due to significant changes in the signal quality depending on the physical Network design.	Prevention oriented Network planning.

Table 2: Classification of Threats

Issue	Categorization
On the basis of resources	1.Passive attack 2.Active attack
Means of attack	1.Transmission/Reception Protocol 2.Control system
On the basis of the target	1.Specific users or network 2.Subnetwork
The intended effect	1. Service disruption 2.Tapping
The location of the attack	1. Terminal 2.Node 3. Link 4. Multiple locations
The attacker's willingness to be discovered	1. Covert 2. Subtle 3.Open

3. Proposed work

The detection study is broken into two parts: an evaluation of the ability of existing fault detection and diagnostic equipment to detect attacks on Optical Networks, and consideration of a new method for detecting certain attacks. There are many reasons for which, in Optical Networks, attacks must be detected and identified at all points in the network where attacks may occur. The speed of attack detection should be commensurate with the data transmission rate of the network. In this work first assume a network than will detect certain types of attacks and possible ways to avoid those applying different algorithms. For this purpose different types of network topology to analyzing the attack can be used. For example 21-node 26-link ARPA-2 network topology is shown below

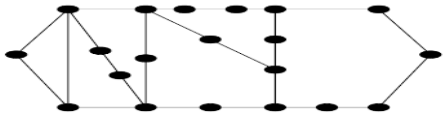

Figure 1: ARPA-2 network

The other network topology can be NsfNet topology (14 nodes), Simple Net topology(4 nodes),INTERNet topology(7 nodes),ARPA-2 network topology(21 nodes).

4. Conclusion

In this review paper attacks in the optical burst switched wavelength division multiplexing network on the basis many measures, several types of attacks have been shown with the counter measures provided to attacks separately.

References

[1] Marija Furdek, "Physical-layer attacks in all-optical WDM networks", IEEE- MIPRO, proceedings of the 34th International Convention, pp. 446 – 451, May 2011.

[2] P.Siva Subramanian and K.Muthuraj, "Threats in Optical Burst Switched Network", International Journal of Computer Technology and Application, Vol 2 (3), pp. 510-514, 2011.

[3] Md. Shamim Reza, Md. Maruf Hossain and Satya Prasad Majumder, "Contention Problem in Optical Burst Switching Network", IEEE-International Conference on Computational Intelligence and Communication Networks(CICN), pp. 239 - 242 , Nov. 2010.

[4] M. Nandi,A. K. Turuk,D. K. Puthal and S. Dutta, "Best Fit Void Filling Algorithm in Optical Burst Switching Networks", IEEE- Emerging Trends in Engineering and Technology (ICETET), 2009 2nd International Conference , pp.609 - 614 , Dec. 2009.

[5] Hongyun Zheng, Changjia Chen, "Performance Analysis of Scheduling Algorithms in Optical Burst Switching(OBS) Networks",IEEE-Innovative Computing, Information and Control, 2007. ICICIC '07. Second International Conference, pp.557 – 557, Sept. 2007.

[6] N. Sreenath, N. Devendra and Balaji Palanisamy, "Reducing Data Loss in Optical Burst-Switched Networks using Adaptive Burst Cloning", IEEE - 15th International Conference on Advanced Computing and Communications, 2007.

[7] J Praveen, B Praveen, and C Siva Ram Murthy, "A First Step towards Autonomic Optical Burst Switched Networks", IEEE-Proceedings of the Second International Conference on Autonomic Computing, pp 94 - 105, Dec. 2006.

[8] Medard et.al, "Attack Detection Methods for All-Optical Networks", IEEE-OFC Technical Digest, pp. 272 – 273, Feb 1998.

(Bhopal, 27 August 1988)Has received B.E degree in Computer science and engineering in 2010 from University, RGPV, and Bhopal, India. Currently undertaking degree in MTECH in Computer science and engineering.