Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 3, March 2017, pg.255 – 260

SECURITY ISSUES IN THE OPTICAL BURST SWITCHED NETWORK: A REVIEW

Palak Kesar

ECE Department, Rayat Bahra University, Punjab, India

palakkesar21@yahoo.in

Mrs. Mandeep Kaur Sandhu

Assistant Professor, ECE Department, Rayat Bahra University, Punjab, India

mandeepcheema@gmail.com

ABSTRACT: - In this review paper the study on the optical burst switched networks has been done. The attacks in the OBS networks and the security issues in the OBS networks explained also. The various types of the security issues and the different types of the features of the OBS networks have been proposed. The main security threat in the OBS networks occurs due to the eavesdropping. The different parameters has been taken such as burst loss ratio, throughput. The implementation of the attack in the networks is done by using network stimulator. In future the work on the denial issues of the security in the OBS has been proposed.

Keywords:- optical burst switching, functions of OBS, security issues.

I. INTRODUCTION

The growth of the internet is increased very quickly and takes place a major role in our life. To provide the better and the easy connectivity we need larger bandwidth that fulfill the demands of the connected users. This bandwidth is also used in industry as well as in the academia [1]. To provide the higher connectivity of the data the internet has switched to optical fiber networks. The optical networks contain a remarkable bandwidth range and the transmission of the data at a rate of average 50 tb/s [2]. To overcome the difficulties that is related to electronics networks architecture and to handle the large growth of the numerous internet users and the bandwidth related applications, optical wavelength division multiplexing (WDM) communications systems are being used in the infrastructure of

the telecommunications industry. The optical communication can transmit data from few tens of megabits to the distance more than kilometer. The advantages of the WDM technology and the continuous growth of the traffic in the internet contains a big mismatch between larger transmission capacity of the optical fiber and routing capability of the electronics routers, which contains the research work on the optical switching technologies:-

1. **Optical Circuit Switching (OCS)**
2. **Optical packet Switching (OPS)**
3. **Optical Burst Switching (OBS)**

OCS is a connection oriented based technology in which a connection is associated already when the data transmission on a predefined light path from the basis to endpoint. OBS is the combination of the optical circuit switching and optical packet switching [2].

OPS execute the packets in which the packets is directed along with the header. The packet is buffered at the node in the optical domain and the header is succeeded with the intermediate node either with optically or electronically [5] . Our main topic of research is OBS.

1. OPTICAL BURST SWITCHING

Optical burst switching networks is used for next generation traffic in a flexible way which is known as OBS. There are mainly two common characteristics in OBS:- First is Client data which contains the assembly and the disassembly at the edge nodes of an OBS network [3]. Second is that the data and control signals are communicated distinctly on different channels and wavelengths [3].

OBS networks is an assembly of connected OBS nodes. The ideologies of OBS networks is the exclusion of the control and data planes by the means of offering the one wavelength for the control planes which uses the electronics switching and other is used in greater part as in the data plane and this mechanism take places in the optical domain [2]. The OBS networks needs a partial delay in the data at middle nodes which certifies useful bandwidth uses on a linking fiber devices.

Functions of OBS networks

OBS contains mainly two types of nodes network:-

EDGE NODE: - It is the interface between OBS NETWORK and client networks EDGE node is again divided into 2 parts: - ingress node and egress nodes [6]. There are mainly six functions of the edge node which are as follow:-

- Burst assembly [6] .
- Burst header packet generation.
- Routing and wavelength assignment.
- Offset computation .
- Burst disassembly
- Signaling

a) CORE NODE: - It is helpful in making the core node of course networks. The core node mainly performs two functions:-

- Scheduling of the resources .
- Contention resolution .

The main functions of the Core node are as:-

- Wavelength conversion .
- Switching speed fast enough .
- Fast optical switching with wavelength conversion and optical buffering.

Architecture of OBS networks

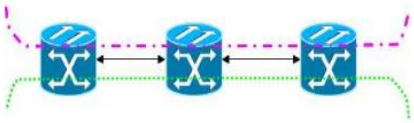

Fig 1:- A simple OBS Network

The basis article of OBS networks is a burst. A burst contains the information which is moving from ingress node to egress node and it shifts from the intermediate nodes [5] . The burst is of two types:- **Control part** which contains header information and sustains control over header [5]. **Payload** used for the transmission of actual data transmission [5].

In OBS the ingress node accumulates the Packets of the internet protocols that are coming from the network of the local access and which is designed to the egress node which is converted into larger variable burst seized burst and is also known as burst assembly [6].

SECURITY IN OBS NETWORKS

The area of security in optical networks is an important issue to handle. The main question which is linked to physical security of networks has to deal with respect to optical networks [4]. Due to the irreplaceable faces of the OBS NETWORK occurs a need for the security openness that is attendant with the burst. A network may be largely categorized into different a field which is based on the goals which are as follows:-

- Traffic analysis [4]
- Eavesdropping
- Data delay
- Service denial
- QOS degradation
- Spoofing
- Burst duplication

There are also various techniques to distribute the attack nomenclature issue and every attack is differentiate by the resources , attack , target, intended effect ,location of attack , last but not the least the attackers enthusiasm. The OBS networks are mostly affected by the eavesdropping [1]. In this threat an aggressor snoops inactively to the verification protocol for capturing the information. This is an issue in OBS when a aggressor attacker intercept the negotiation burst of the data. The burst of data is the main topic of the attack the inactive aggressor is able to analyze and detects the traffic information from the burst header. In OBS, inactive Aggressors are very difficult to detect there are many prevention methods that can be used to pledge the attack and the threat. The planned solution for the security is Control Packet Protection (CPPT-OBS), in this three cases was investigated [1]. The following three cases are: OBS network lacking security measures and lacking security attacks, OBS network under security attacks lacking security measures, and finally OBS network under security attacks with security measures .

In the OBS networks edge node and core nodes are valid nodes. Under this negotiation, each node is equipped with security measures such as privacy and authentication using RSA encryption algorithm. This process is called self-controlling. The RSA encryption is used to encrypt and decrypt burst control packets. The source and destination are point-to-point connected to each other. The security works on the following issues which are as follows:-

Burst Duplication Attack :- In OBS network, for every burst of data a consistent control burst will be generated by the ingress source node and sent forward with an offset time interval. They will travel complete the intermediate core nodes and finally reach the egress edge node[1]. The arrangement of necessary capitals will be completed by the intermediate core nodes with the help of the control burst.

Counter measure: - In this the duplication of the burst can be detected and there are two methods to detect the duplication of the burst. The first method uses the digital sign to sense and eliminate the spell which is based on digital signature and the control burst is protected from unofficial modification due to which the burst duplication attack in the OBS networks can be prevented and which is achieved by using the per hop burst header validation in every intermediate core router [1]. and in the second method the reliable node will be used to detect and eliminate the attack and this approach is better than the digital signature because of the overhead feature and the time required for the detection of the attack and this node is useful for govern the performance of the core node.

II. Related Work

Yahaya Coulibaly et al. [1] explain Secure Burst Control Packet Scheme for Optical Burst Switching Networks. In this paper, they propose and evaluate a solution to address Data Burst Redirection (DBR) Attack in OBS networks. The solution was designed based on Rivest-Shamir-Adleman (RSA) public-key encryption algorithm. They evaluated the algorithm via computer simulation. Evaluation metrics are burst loss ratio and throughput. The obtained results demonstrate that, the proposed algorithm had succeeded in protecting the network against DBR attacks reducing the number of compromised BHP. Maninder Lal Singh et al. [2] explain Review of optical burst switching. In this paper they present an emerging technology of optical communication. In they compare this new emerging technology with the pre-existing switching paradigms like OCS and OPS. This review article completely explains the various mechanisms related to OBS like burst assembly, wavelength reservation, burst scheduling and contention resolution. They concluded that Optical Burst switching is a very promising communication technique in

fiber communication. And it is acquire the whole communication market in the few years. Yang Chen et al. [3] explained A New Area in Optical Networking Research. In this paper they explained the Basic burst assembly algorithms and their effect on assembled burst traffic characteristics. Then they explained a brief review of the early work on burst transmission which is followed by the fundamental protocol known as JUST – ENOUGH – TIME. Evaluation metrics are tradeoff and their implementation. Siddharth Singh chouhan et al. [4] explained Identification of current attacks and their counter measures in Optical burst switched networks. In this paper they identify potential threats of the security in the OBS networks. In this they purpose different networks topology to detect the attack on the network. They explained attack in the optical burst wavelength division multiplexing network on the base of its measures different attacks. Md. Shamim Reza et al. [5] explained Performance Analysis of an (OBS) Network. They explained that a burst loss rate (BLR) scheme suitable for slotted optical burst switched networks. In this paper they represented an analytical model of a burst loss rate scheme for slotted burst of an optical burst switching. The effects of several network design parameters on the system performance measures have been investigated and presented numerically. They demonstrate the system performance that improves the no of increasing wavelength and the conversing of the wavelength capability that reduces the network traffic and the proability of the block burst increases.

Muhammad Shafie Abd Latiff et al [6] QoS Performance Analysis of Non-slotted and Slotted Optical Burst Switched Networks. They explained focus on architectural solutions where they investigate QoS performance of non-slotted and slotted OBS in terms of burst loss ratio and throughput.in this they explains the Hierarchical Time Sliced was proposed in OBS to address an important issue in slotted OBS. The evaluation of QoS performance of slotted OBS represented by Hit SOBS and a non-slotted OBS network was carried out by them. P. Siva Subramanian et al. [7] explained Threats in Optical Burst Switched Network. In this paper they explained the threats in security issues and the counter measures that occur in the OBS networks. They categorize the burst duplication attack and find the two different methods to diminish the burst stealing attack.

III. Conclusion

In this review paper concluded the introduction of the optical burst switching networks and the security issues in the OBS networks. The network topology used to find out the security attack in the OBS networks by using the software network stimulator. In future, the work on the issues of denial of service which covers the reliability aspects and the expected result may contains the end-to-end delay that may be increased due to the security amount that may planned and this method can be used to enhanced the address of the delay issue. Different parameters have been taken to evaluate the security issues.

References

[1]. Coulibaly, Yahaya, et al. "Secure burst control packet scheme for Optical Burst Switching networks." Broadband and Photonics Conference (IBP), 2015 IEEE International. IEEE, 2015.

[2]. Muhammad Shafie Abd Latiff et al. "QoS Performance Analysis of Non-slotted and Slotted Optical Burst Switched Networks". 2015 IEEE 12th Malaysia International Conference on Communications (MICC).

[3]. T. venkatesh et al. " An analytical approach to optical burst switched networks ". Springer Verlag 2010

[4]. Md. Shamim Reza et al. et al. "Explain a burst loss rate (BLR) scheme suitable for slotted optical burst switched networks." 5th International Conference on Electrical and Computer Engineering ICECE 2008, 20-22 December 2008.

[5]. P. Siva Subramanian et al. " Threats in Optical Burst Switched Network" Int. J. Comp. Tech. Appl., Vol 2 (3), 510-514.

[6]. Maninder Lal Singh et al." Review of optical burst switching. International Journal of Engineering Sciences & Research Technology. IJESRT, 4(10): October -2015

[7]. Yang Chen et al. "A New Area in Optical Networking Research.

[8]. Siddharth singh chouhan et al. "explain Identification of current attacks and their counter measures in Optical burst switched networks.

[9]. C.Qiao and M.Yoo "Optical burst switching (OBS)-A new paradigm for an optical internet," Journal of High Speed Network, vol. 8, no. 1, pp. 69-84, Jan. 1999.

