Security Issues and the Energy Consumption in the Optical Burst Switched Networks

Palak Kesar[1], Mandeep Kaur Sandhu[2]

[1]Research Scholar, [2]Assistant Professor
[1,2]ECE Department, Rayat and Bahra University, Mohali, Punjab, India

How to cite this paper: Palak Kesar | Mandeep Kaur Sandhu "Security Issues and the Energy Consumption in the Optical Burst Switched Networks" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-4, June 2019, pp.881-885, URL: https://www.ijtsrd.com/papers/ijtsrd23934.pdf

IJTSRD23934

ABSTRACT

Optical burst switching is an optical network technology that helps in improving the use of the optical networks resources. In OCS, the network is configured to establish a circuit, from an entry to an exit node, by adjusting the optical cross connects circuits in the core routers in a manner that the data signal, in an optical form, can travel in an all-optical manner from source to destination node. This approach suffers from all the disadvantages known to circuit switching - the circuits require time to set up and to destroy, and while the circuit is established, the resources will not be efficiently used to the unpredictable nature of network traffic. Security is one of the major problems in field of networks. Mainly this work focused on security issues in optical burst switching and to decreased the energy consumption. In this research work, a secure public key cryptography technique is proposed and evaluated as a security solution to measure security threats related to burst packet in optical burst switching networks.

Keywords: *WDM, OCS, OBS, MPLS, BGP*

Introduction

With recent advances in wavelength division multiplexing (WDM) technology, the amount of raw bandwidth available in fiber links has increased by many orders of magnitude. Meanwhile, the rapid growth of Internet traffic requires high transmission rates beyond a conventional electronic router's capability. Optical fibers are found to the solution of this increasing demand. There are numerous advantages of fibers include security, no interference, and lower errors in addition to enormous bandwidth. Initially, fibers were used for point-to-point communication where the full capacity of the fiber was not utilized [1]. Optical network is considered as the optimal choice for the next generation high speed network due to potentials and benefits of optical components particularly its carrier i.e. optical fiber [2].Optical fibers have the capability to transmit Tbps range of data. After the successful research of the optical fiber several optical network paradigms for future Internet backbone have been under intensive research. Optical switching techniques have great impact on the performance of the optical network. Although there are many advantages a well disadvantages of these optical switching paradigms. There are mainly three types of the switching paradigms that are used which are as follows:-

1. Optical circuit switching (OCS).
2. Optical packet switching (OPS).
3. Optical Burst switching (OBS).

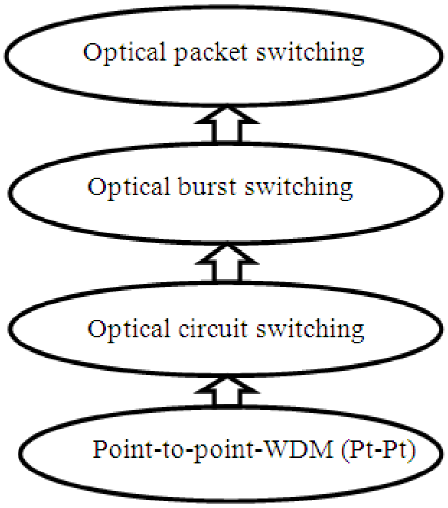


Fig. 1.1 Evolution of the switching techniques

Optical circuit switching:-OCS is a connection oriented switching technique in which a connection is set up before actual data transmission on a pre-defined light path from the source to the destination [3].In OCS, the network is configured to establish a circuit, from an entry to an exit node, by adjusting the optical cross connects circuits in the core routers in a manner that the data signal, in an optical form, can travel in an all-optical manner from the entry to the exit node. This approach suffers from all the disadvantages known to circuit switching - the circuits require time to set up and to destroy, and while the circuit is established, the resources will not be efficiently used to the unpredictable nature of network traffic. Large connection set up time and low bandwidth utilization in case of low traffic load are the major limitations of the OCS.

Optical packet switching:-In OPS, a packet comprises data and a header which are in optical domain. When the packet comes at the core node, the header is extracted from the packet and is converted into the electrical domain for processing. The data in the packet has to be buffered in the core node during header processing.

Optical burst switching:-OBS is the combination of the optical circuit switching and optical packet switching. The OBS is an upcoming network that has stroke a perfect balance between the finely grained packet switching and the coarse grained circuit switching. Optical burst switching is an adaptation of the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) which is also known as a standard for burst switching in ATM networks, which is commonly known as ATM block transfer (ABT). There are two versions of ABT: ABT with delayed transmission and ABT with the immediate transmission.

Security issues in the OBS networks: Some of potential threats in OBS network such as traffic analysis, eavesdropping and spoofing and burst duplication attack and service disruption via Denial of Service (DoS) [14]. During transmission, the scheduling request during transmission, the scheduling request for a BHP may be rejected due to overflowing demands and the corresponding data burst is disconnected thus becoming an Orphan Burst [8]. These burst may flow along an unintended path wasting the bandwidth or even be tapped by an attacker compromising the security. The various security issues in the OBS networks are as follows:-

1. Traffic analysis [14].
2. Eavesdropping.
3. Data delay.
4. Service denial.
5. QOS degradation.
6. Spoofing.
7. Burst duplication attack.

But the OBS are mostly affected by the traffic analysis, Eaves dropping and Burst duplication. This is the main threats of the OBS networks which affects the transmission of the packets while transmission.

Multi-protocol label switching:-MPLS was intended by Internet Engineering Task Force (IETF).Multi-protocol label switching is a switching technology which is used by the different service providers to enhance and boost up the traffic and to increase the overall performance of the system. MPLS is mainly used by the providers to enhance the quality of the service. MPLS uses the different protocol to transfer the packets from one node to another node so it is also known as " Multi-protocol' 'MPLS is a connection –oriented approach which meant to transmitted the data packets from sender to the receiver by using a preliminary protocol before sending the data Multi-Protocol Label Switching is a method that directs data from one system node to the next based on short path labels rather than long network addresses in high-performance telecommunications association. MPLS offers high scalability, end-to-end IP services which contains simple configuration and management for customers as well as to the service providers. It forwards packets in any system protocol, which are mainly known as building blocks of data transmitted over the Internet. Each packet has a header. In a non-ATM contextual, the packet's header contains 20-bit label which contains 3-bit of the class of service and 1-bit of the label stack but in the case of the ATM contextual, the packet's header contain only Virtual Channel Identifier/Virtual Packet Identifier encoded label. These labels reduce the time of a router to search for the address to next node to forward packet.

A MPLS enabled Internet consists of a set of nodes called Label Switch Routers (LSRs) and Label Edge Routers (LERs). The LERs and LSRs are capable of switching and routing packets through multiple paths called Label Switched Paths (LSPs). LSPs are formed on the basis of a label which has been appended to each packet instead of the Internet Protocol (IP) address. The LERs present at the beginning edge of the MPLS domain are called ingress nodes and the LERs at ending edges of the MPLS domain are called ingress nodes [3]. Load balancing is realized in MPLS networks by redistributing the traffic over two or more LSPs, which connect the same ingress and egress node pair. MPLS works by prefixing packets with an MPLS header having one or more label known as label stack. With the contribution of MPLS-capable routers or switches in central gateway protocols such as Open Shortest Path First (OSPF) or Intermediate System to Intermediate System (IS-IS), the network automatically builds routing tables. Label Distribution Protocol (LDP) uses this table to establish label values between neighboring devices [13].

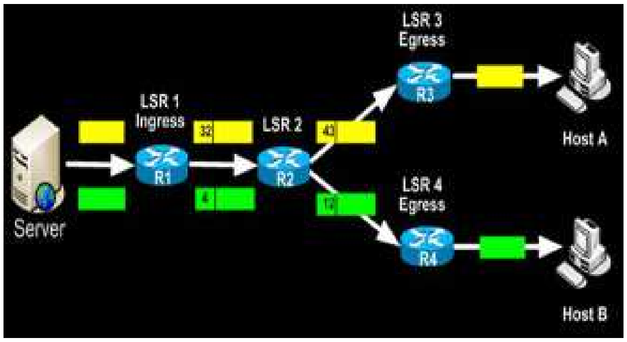


Fig. 1.11 Block diagram of MPLS

3.1 Border gateway protocol:

Border gateway protocol is the most important protocol of the Multi label switching technique. The Border Gateway Protocol (BGP) is an inter-autonomous system protocol. BGP runs over any reliable transport level protocol. TCP will be used, however, since it is present in virtually all commercial routers and hosts. The primary function of a BGP system is to exchange network reachability information with other BGP systems. This network reachability information includes information on the autonomous systems (AS's) that traffic must transit to reach these networks [28]. This information is sufficient to construct a graph of AS connectivity from which routing loops may be pruned and policy decisions at an AS level may be enforced. BGP is actually two protocols - iBGP, designed for internal routing, and eBGP, designed for external routing. The routers which provide the interface between domains run a protocol called Border Gateway Protocol (BGP). Figure 1 shows a high-level abstraction of BGP routers connecting up domains in the Internet. Each local routing domain is called an Autonomous System (AS)[24].

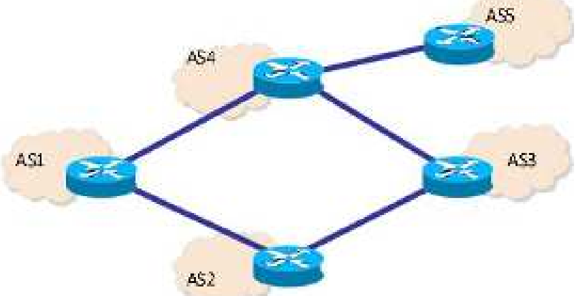
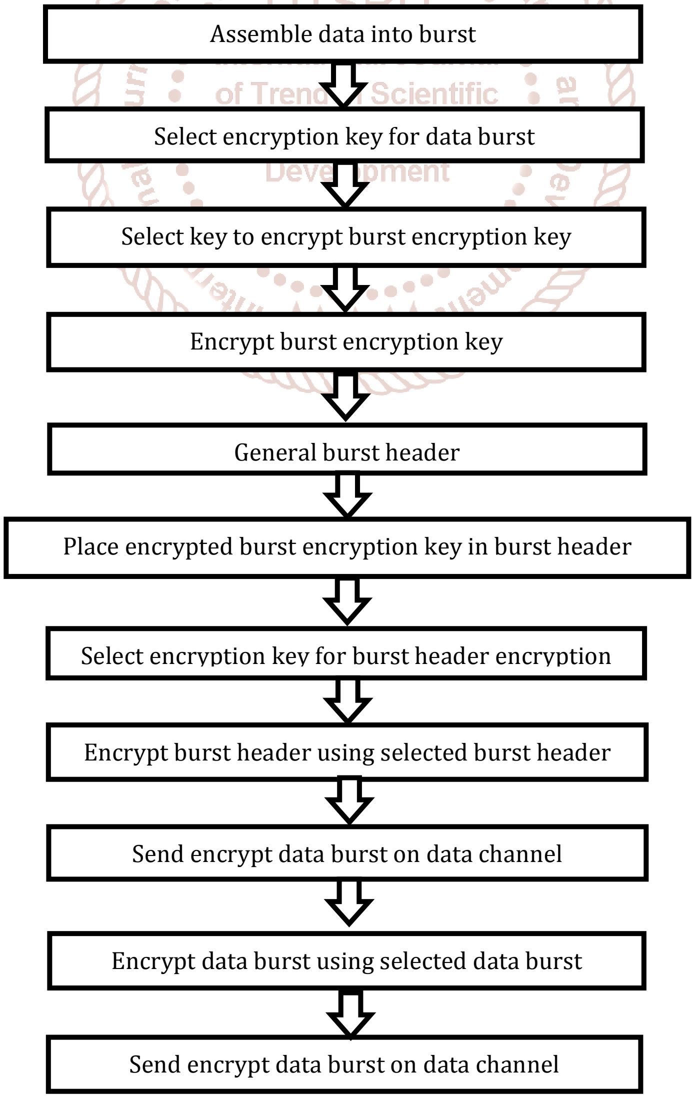


Fig.1.2 BGP routers

Proposed Methodology: Optical burst switching is an optical network technology that helps in improving the use of the optical networks resources. In the previous work, the authors focus on architectural solutions where they investigate QoS performance of non-slotted and slotted OBS in terms of burst loss ratio and throughput. The value of the BLR in the previous paper is very much high so to solve this problem we use the MPLS technique with the help public key Cryptography. To avoid these security issues in the optical burst switched networks the multi-protocol label switching technique used for improving these issues the public key cryptography algorithm use in the proposed use.


Assemble data into burst
Select encryption key for data burst
Select key to encrypt burst encryption key
Encrypt burst encryption key
General burst header
Place encrypted burst encryption key in burst header
Select encryption key for burst header encryption
Encrypt burst header using selected burst header
Send encrypt data burst on data channel
Encrypt data burst using selected data burst
Send encrypt data burst on data channel

Firstly, the number of the nodes collapse with each other to form a network after that the nodes of the networks are able to start transferring the data to start the communication between the sender to the receiver select the transmitted node number and the receiver node after then the transmitter will find out the shortest path for sending the data packets from sender to the receiver.

A. After the path in a particular region the data packets are assemble in a particular form in the form of burst.
B. Then encrypt the data by converting it into byte code so that it can be readable only for the receiver.
C. Assign burst a key which is the receiver id if these key matches with the receiver only then it will decrypt the data.
D. After encryption it will sends data to the receiver node.
E. Then assign header to the each burst.
F. Assigns the burst encryption key to the burst header.
G. Also assigns the burst header a unique key for its identity.
H. Encrypt the burst header so that no one can read it for security purpose.
I. Send the burst header to the control channel.
J. The receiver decrypt the data burst when the key matches.
K. After the key matches the receiver sends the ack to the sender and after then the communication starts.

Algorithm used in the proposed work

```
Encrypt the data by converting it into byte code;
attach pK to packet ; (where pK==private Key)
send the packet through the route;
if (receiver id == pK)
{
    decrypt the data;
    send positive response ;
}
else
    data remains encrypted;
if (sender doesn't get the response)
    it sends another packets through another route;
```

Results analysis:-

In this section, the results of the proposed and the existing techniques are defined and also the comparison of the existing results and the proposed work is explained. In the existing paper the researchers introduces QoS Performance Analysis of Non-slotted and Slotted Optical Burst Switched Networks. They had taken two different parameters taken Burst loss ratio and throughput. The evaluation of QoS performance of slotted OBS represented by Hierarchical Time Sliced (Hit SOBS).

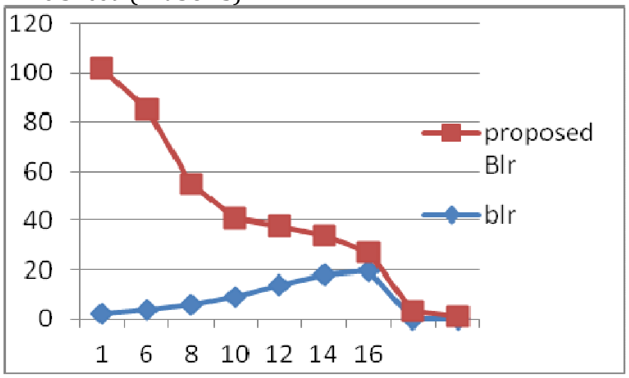


Fig.5.1 Comparison of both existing and proposed Burst loss ratio

Fig. 5.1 explains the burst loss ratio in which the X-axis represents time and Y-axis represents burst loss. Red line represents BLR. As a time increases BLR also increases.

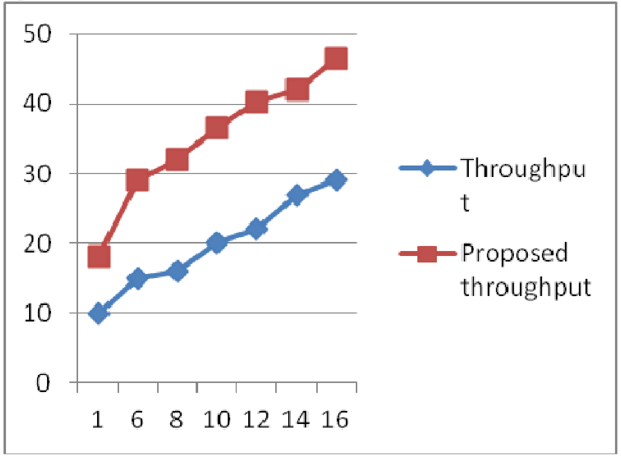


Fig. 5.2 Comparison of both existing and proposed Throughput

Fig. 5.2 explains throughput. Where X-axis represents time and Y-axis represents throughput. Throughput increases with time in this graph.

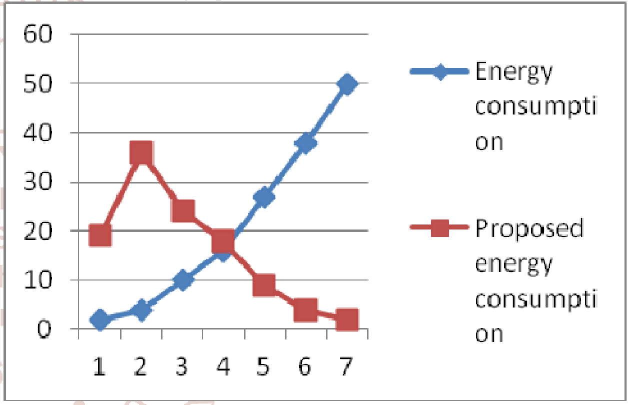


Fig. 5.3 Comparison of both existing and proposed Energy consumption

Fig. 5.3 explains the energy where X-axis represents time and Y-axis energy. In this graph energy consumption decreases due to secure encryption technique.

Conclusion:

Optical circuit switching is a connection oriented switching technique in which a connection is set up before actual data transmission on a pre-defined light path from the source to the destination. 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 optical burst switching network, there is a degree of security vulnerability associated with the burst. Security is one of the major problems in field of networks. Mainly this work focused on security issues in optical burst switching and decreased the energy consumption. In this research work, a secure public key cryptography technique is proposed and evaluated as a security solution to measure security threats related to burst packet in optical burst switching networks. NS2 simulator is used for implementation purpose. It is analyzed that proposed solution provides better results under attack environment that will reduce the burst loss and increase overall network throughput.

Future work:-

In future, proposed technique can be implemented on other protocols such as RSVP and LDP to improve its security. By using the Border gateway protocol on the other switching paradigms ie; optical circuit switching as well and the optical packet switching the security issues in these parameters also improved and also by using the different parameters the energy consumption of the networks also decreased. Moreover, other security issues also improved by using the MPLS.

References

[1] Baldine, G.N. Rouskas, H.G. Perros, and D. Stevenson, "JumpStart: A Just-in-Time Signaling Architecture for WDM Burst-Switched Networks," IEEE Communications, vol. 40, no. 2, pp. 82-89, Feb. 2002.

[2] Phuritatkul, Jumpot, Yusheng Ji, and Shigeki Yamada,"Proactive wavelength pre-emption for supporting absolute QoS in optical-burst-switched networks," Journal of Light wave Technology 25.5 pp.1130-1137, 2007.

[3] Y. Chen, C. Qiao and X. Yu, "Optical burst switching: A new area in optical networking research," IEEE Network Magazine, Vol. 18, no. 3, pp. 16-23, May 2004.

[4] Y. Xiong, M. Vanderhoute, and H.C. Cankaya, "Control Architecture in Optical Burst-Switched WDM Networks," IEEE Journal on Selected Areas in Communications, vol. 18, no. 10, pp. 1838-1851, Oct. 2000.

[5] Siddharth Singh Chouhan and Sanjay Sharma, "Identification of current attacks and their counter measures in optical burst switched (OBS) network." International Journal of Advanced Computer Research volume 2, issue 3, March 2012.

[6] Vokkarane, Vinod M., Jason P. Jue, and Sriranjani Sitaraman. "Burst segmentation: an approach for reducing packet loss in optical burst switched networks." In Communications, IEEE International Conference on, vol. 5, pp. 2673-2677, May 2002.

[7] X. Yu, Y. Chen, and C. Qiao. "Study of traffic statistics of assembled burst traffic in optical burst switched networks". In Proc. Opticomm, vol. 4874, pp. 149-159, July2002.

[8] Y. Coulibaly, A. A. I. Al-Kilany, M. S. A. Latiff, G. Rouskas, S. Mandala, and M. A. Razzaque. 'Secure burst control packet scheme for Optical Burst Switching networks''. In Broadband and Photonics Conference (IBP), IEEE International pp. 86-91, April 2015.

[9] Coulibaly, Y., Latiff, M. S. A. Umaru, A. M, & Garcia, N. M, "QoS performance analysis of non-slotted and slotted optical burst switched networks'', IEEE 12th Malaysia International Conference., In Communications (MICC), pp. 153-156, November 2015.

[10] T. F. Fernandez and, C. N. Sreenath "Burstification threat in optical burst switched networks". In IEEE proceeding of International Conference on Communication and Signal Processing, pp. 1666-1670, April 2014.

[11] J. Choi, H. L Vu, and M. Kang "On achieving the optimal performance of FDL buffers using burst assembly". IEEE Communications Letters, vol.11, issue11, November, 2007.

[12] F. Yu, Huang, M., J., Zhang, and X. Sun, 2005 August. "A contention resolution scheme by using fiber delay lines for optical burst switching." In Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications, MAPE IEEE International Symposium on vol. 2, pp. 1287-1290, August, 2005.

[13] X. Yu, Y. Chen and C. Qiao "Study of traffic statistics of assembled burst traffic in optical burst switched networks". In Proc. Opticomm Vol. 4874, pp. 149-159, July, 2002.

[14] F. Farahmand and J. P. Jue, "Look-ahead Window Contention Resolution in Optical Burst Switched Networks," IEEE Workshop on High-Performance Switching and Routing (HPSR) 2003, pp. 147-151, Torino, Italy, June 2003.

[15] S. Yao. S.J. Ben Yoo, and B. Mukherjee, "A Comparison Study between Slotted and Unslotted All-optical Packet Switched Network with Priority-Based Routing," Proceedings, Optical Fiber Communication Conference and Exhibit (OFC), vol. 2, 2001.

[16] Niladhuri Sreenath, Fernandez, Terrance Frederick, and Brabagaran Karunanithi "Spectral threats in TCP over optical Burst switched networks." IEEE proceeding of 1st International Conference on Trends for Technology and convergence, Salem, Tamil Nadu, India (2014).

[17] Y. Xiong Zheng, M. Vandenhout, and H. C. Cankaya, "Hardware Design of a Channel Scheduling Algorithm for Optical Burst Switching Routers," Proceedings, SPIE ITCOM 2002, vol. 4872, pp.199-209, 2000.

[18] R. Ramaswami and K. N. Sivarajan, "Routing and wavelength assignment in all-optical networks," IEEE/ACM Trans. Network, vol. 3, no. 5, pp. 489–500, Oct. 1995.

[19] P. Siva Subramanian and K. Muthuraj, "Threats in optical burst switched network." Int. J. Comp. Tech. Appl., vol. 2 issue 3, pp.510-514, 2011.

[20] Alouneh, S., Abed, S. E., Kharbutli, M., & Mohd, B. J,'' MPLS technology in wireless networks. Wireless networks, Springer, vol. 20, issue 5, pp.1037-1051, November 2013.

[21] K.K.Nguyen & B.Jaumard, "A MPLS/LDP Distributed architecture for Next Generation Routers," Springer, vol. 21, issue 4, pp. 535–561, December 2013.

[22] T. Usui, Y. Ketatsiyi, H.Yokota, ''A study on traffic management cooperating with IMS in MPLS", Springer, volume 52, .issue 2, pp. 671-680, February 2013.

[23] Acharya, A. Ganu, S. Misra, A., "DCMA A Label Switching MAC for Efficient packet Forwarding in Multihop Wireless Network", Selected Areas in Communications, IEEE Journal, vol. 24 on 11, pp. 1995-2004, Nov. 2006.

[24] A. S. Acampora and I. A. Shah, "Multihop light wave networks: A comparison of store-and-forward and hot-potato routing," IEEE Transaction on Communication, vol. 40, no. 6, pp. 1082–1090, Jun. 1992.