# SPECTRAL THREAT IN TCP OVER OPTICAL BURST SWITCHED NETWORKS

**Terrance Frederick Fernandez[1], Brabagaran Karunanithi[2], Sreenath Niladhuri[3]**

[1]*Research Scholar, Computer Science and Engineering, Pondicherry Engineering College, Puducherry, India*
[2]*M.Tech Student, Computer Science and Engineering, Pondicherry Engineering College, Puducherry, India*
[3]*Professor, Computer Science and Engineering, Pondicherry Engineering College, Puducherry, India*

## Abstract

*Exponential increase in the number of online users has increased over the years posed a demand for high speed core architecture for the internet. The Optical Burst Switching (OBS) is a new switching architecture that efficiently utilizes the bandwidth of the optical layer. It offers all-optical switching as there is no Optical-Electronic conversion at any intermediate switching node. It is one of the three optical switching architectures, while others being Optical Circuit Switching (OCS) and Optical Packet Switching (OPS). The basic switching entity of OBS is a burst which posses an intermediate granularity between a packet and the amount of optical data in a circuit. The OBS architecture merits the shortcomings of the other two optical architectures namely OCS and OPS. This efficient core networking architecture, suffers from various security vulnerabilities. This paper proposes a novel security threat namely the spectral threat. It is a threat that affects only multicast capable nodes. Multicast Capable nodes are those nodes that are capable of multicasting an optical data. The wavelength of the optical data burst is altered resulting in flooding of data to a particular outgoing channel and ultimately blocking the channel. The attack results in losses thereby reducing the burst throughput and increasing the burst latency. The paper further summarizes other potential threats affecting normal nodes and Multicast Capable nodes for TCP over OBS networks.*

***Keywords:*** *Optical communication, Optical Burst Switching, Vulnerabilities in OBS Networks and Spectral Threat.*

----------***----------

## 1. INTRODUCTION TO OPTICAL BURST SWITCHING

Driven by the demand to achieve huge bandwidth, the researchers wanted a cost effective optical networking architecture at the cores [1]. The optical circuit switching architecture is cozy to build, yet lacks flexibility to cope with the bursty internet traffic. Though optical packet switching poses a theoretically ideal architecture, it still suffers from immaturity in optical buffers. On the other hand, people from academia find the Optical Burst Switched architecture feasible as the future technology for the network cores [2], [3].

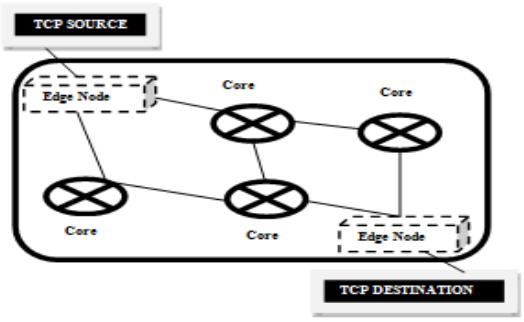


**Fig -1**: OBS Architecture

In OBS, packets from different sources belonging to same destination are aggregated into a Burst and are forwarded through the cores, to the destination. OBS architecture is given in Figure 1. Unlike others, these Bursts do not contain control information. Instead there is a burst header packet, which carries control data for an associated data burst. A typical BHP format is shown in Figure 2.

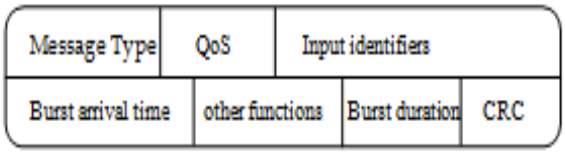


**Fig -2**: Burst Header Packet (BHP) format

The header undergoes O/E/O conversion at the intermediate nodes for processing, while its burst is transmitted all-optically. The expected total processing time by a header packet is calculated and it is called offset time, after which the data bursts for the corresponding headers are sent [4]. Since the burst transmission at the cores is entirely at the optical domain and with the absence of potential optical buffers, there is a possibility of two or more bursts contend at the same outgoing channel and at the same instant. This phenomenon is

called as Burst Contention. There are a number of resolution mechanisms available like wavelength conversion [5], segmentation [6], optical buffering [7] and deflection routing [8].

## 2. OPTICAL NODE CLASSIFICATION

Since Optical Burst Switched Networks are all-optical in nature, multicasting is not possible in every core node due to absence of potential Optical buffering technology. Based on an optical node capability, the classification is [9]:

### 2.1 Multicast Capable Optical Cross-Connect Switches (MC-OXC)

As discussed in Section 1, the BHP undergoes O/E/O conversion at the cores while the DB is all-optical. In order to split an incoming Burst all-optically, an optical node must possess light-splitting capability. Such nodes come under Multicast Capable nodes.

### 2.2 Multicast Incapable Optical Cross-Connect Switches

Other nodes that do not posses sufficient capability to multicast a Data Burst all-optically come under the Multicast Incapable nodes.

## 3. VULNERABILITIES IN OBS NETWORKS

Apart from being troubled in contention as discussed in Section1, OBS suffers from security threats too. 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 [10].

The orphan bursts may flow along an unintended path wasting the bandwidth or even be tapped by an attacker compromising the security. Sometimes the BHP may be modified thus compromised by fraudulent parties forming Malicious Burst Headers and these include Time-out attack, Replay attack, Flooding attack and Burst Hijacking.

Time-out attack happens when an attacker allegedly modifies the time-out field on the BHP. The time-out field is used for timer based assembly mechanism [11]. When this value is changed, bursts of shorter length are formed causing lot of unwanted mice flows in the network.

In replay attack [10], a compromised node makes copy of BHP and stores it. In later time or in some other day, compromised node injects this BHP illegally that will get its channel allocated. In a flooding attack [12], the compromised node creates multiple copies of the BHP and forwards it to the next node and thereby flooding with duplicate copies of BHP.

In order to make reservations for these bogus bursts the resources are blocked and denied for valid bursts. The compromised node tunnels the BHP to the attacker and it is called Burst hijacking [13]. The above vulnerabilities do not happen at a multicast OBS node and there are certain other vulnerabilities that could happen at the Multicast Capable nodes and they include Burst Duplication and Land attack.

The duplication attack is similar to hijacking except for the fact it exploits the multicast node capability. The compromised node also splits the Burst along with its header and transmits it to the attacker. In land attack [14], the compromised node copies the BHP, transmits back to the source as well as to the intended destination. Since the attack is on a MC node, the payload also gets split and reaches both intended and unintended nodes thereby wasting resources.

## 4. SPECTRAL THREAT FOR OBS NETWORKS

As seen from the BHP format in section 1, there is an input wavelength field specified for a corresponding burst. The attacker may compromise a core node and then change the wavelength of an incoming burst. Thus it may send it to an unintended channel. It may even change all incoming BHP to one particular channel thereby leading to contention. Since this particular attack takes place in spectral/wavelength domain it is called as spectral attack. This threat is shown in figure 3.

The network supports three wavelengths (say λ1, λ2 and λ3) which are shown as three lines in the figure. The attacker compromises the node 3. The IP packets are initially assembled and sent as burst to the ingress, where individual channels are allocated to each formed burst. These are now forwarded to the compromised node 3, where all incoming bursts are altered to one wavelength (λ3).This causes contention at the next core node 9. To resolve contention, resources may be wasted or other routes are considered that are not optimal. The overall throughput decreases due to this attack.

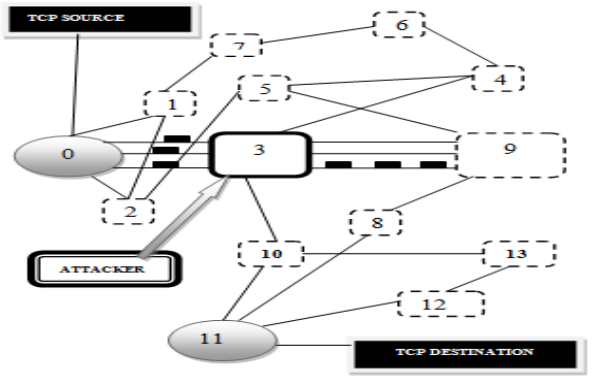


**Fig -3**: Spectral Attack on a core node in TCP over OBS networks

## 5. SIMULATION RESULTS

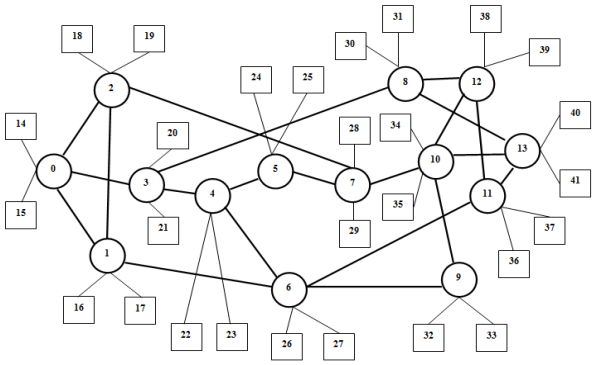


**Fig -4**: NSFNet Topology

The left side of the table denotes the simulation Parameters and the right side denotes the values of the same. Link speed of the optical channel is given in Giga bytes. The simulation time and the switching time is given in milliseconds (ms). All the other network simulation parameters carry default values.

**Table -1:** Simulation Parameters

| Parameter | Value |
|---|---|
| Number of Electronic nodes | 28 |
| Number of Optical nodes | 14 |
| Link Speed | 1 GB |
| Simulation Time | 60 ms |
| Switching Time | 0.001 ms |

This attack is simulated in ns2 with modified nOBS patch [15] in a 14 node NSF network with the simulation parameters given in Table 1. Burst throughput before and after spectral attack acting upon Multicast Capable and normal nodes are shown in Chart 1, 2 and 3.

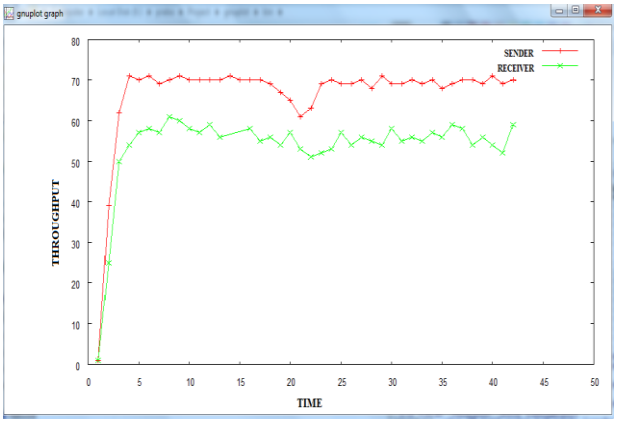


**Chart -1**: Throughput Vs Simulation Time (Normal Multicast Incapable Nodes)

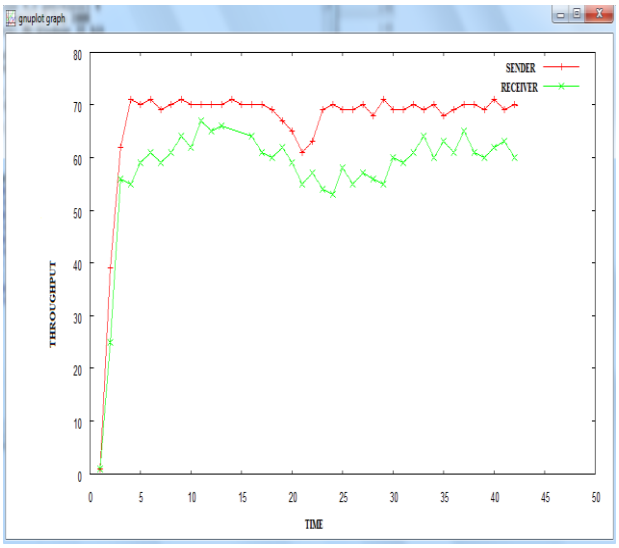


**Chart -2**: Throughput Vs Simulation Time (Normal Multicast capable Nodes)

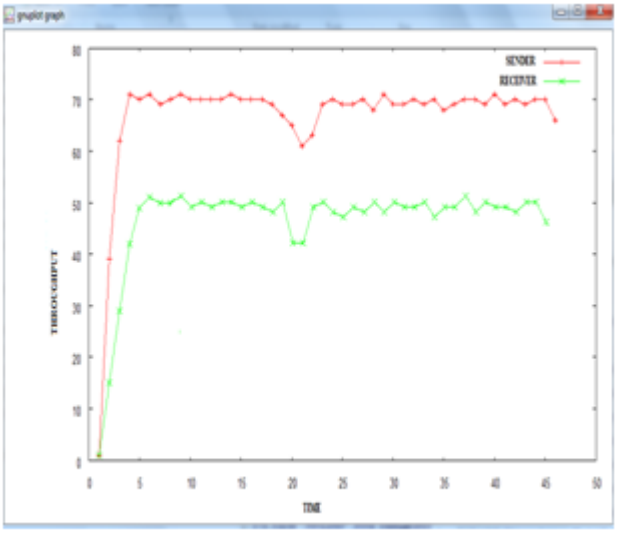


**Chart -3**: Throughput Vs Simulation Time (After Attack on Multicast capable Nodes)

## 6. CONCLUSIONS

The paper reviews various security vulnerabilities in an OBS network and proposes a novel threat happening in the wavelength domain. The effect of this security compromise shown before and after attack proves the lethality of the same on an MC node in comparison with a normal node. Multicast Capable nodes must be secured well as the effect of MC node compromise will be higher than a normal node compromise. The optimized route configured during light-tree configuration phase is not taken when a particular node is compromised thus wasting network resources. The quantification of the above

discussed are considered as the future work to this proposal.

## REFERENCES


[1] Md. Shamim Reza, Md. Maruf Hossain and Satya Prasad Majumder, "Contention Problem in Optical Burst Switching Network", International Conference on Computational Intelligence and Communication Systems, pp 239 – 242, 2010. (Conference proceedings)

[2] Y. Xiong, M. Vandenhoute, and H. Cankaya, "Control architecture in optical burst-switched WDM networks," IEEE Journal of Selected Areas in Communication, vol. 18, no. 10, pp. 1838–1851, Oct. 2000. (IEEE Journal)

[3] J. Ramamirtham and J. Turner, "Time sliced optical burst switching", Proceeding of IEEE computer and communications, vol.3, pp. 2030–2038, 2003. (Conference proceedings)

[4] H. M. H. Shalabi, " A simplified performance analysis of optical burst switched networks." Journal of Lightwave Technology, vol. 25, no. 4,pp. 986-995, April 2007. (Journal citation)

[5] B. Ramamurthy and B. Mukherjee, "Wavelength conversion in WDM networking", IEEE Journal of Selected Areas in Communication, vol. 16, no. 7, pp. 1061–1073, 1998. (IEEE Journal citation)

[6] V. Vokkarane and J. Jue, "Burst segmentation: An approach for reducing packet loss in optical burst switched networks", SPIE Optical Network Magazine, vol. 4, no. 6, pp. 81–89, Nov.–Dec. 2003. (Magazine citation)

[7] .Y.Choi, H.L.Vu and M.Kang, "On Achieving the Optimal Performance of FDL Buffers Using Burst Assembly", IEEE Communication Letters, vol. 11, no. 11, pp- 895-897, November 2007. (Communication Letters)

[8] X. Wang, H. Morikawa, and T. Aoyama, "Burst optical deflection routing protocol for wavelength routing WDM networks", in Proceeding of SPIE Optical Network Communication Conference, pp. 257–266, October 2000. (Conference proceedings)

[9] B. G. Bathula, V. M. Vokkarane, and R. R. C. Bikram, "Impairment aware manycasting over optical burst-switched (OBS) networks," in Proceeding on International Conference on Communications, pp. 5234–5238, May 2008, Beijing, China. (Conference proceedings)

[10] Yuhua Chen, Pramode K. Verma, "Secure Optical Burst Switching: Framework and Research Directions", IEEE Communications magazine, vol.46, no.8, pp. 40-45, August 2008. (Magazine citation)

[11] N.Sreenath, K.Muthuraj, N.Ramkumar , "Secure Optical Internet : A novel threat detection and its countermeasures", in proceeding of International Conference on Electronics and Embedded Systems, 2012. (Conference proceedings)

[12] K. Muthuraj and N. Sreenath, "Secure Optical Internet: An attack on OBS node in a TCP over OBS Network", International Journal of emerging trends and technology in computer science, vol.1, no.4, pp.75-80, December 2012. (Journal citation)

[13] K.Muthuraj and N.Sreenath, "Secure Optical Internet: A novel attack prevention mechanism for an OBS node in TCP over OBS networks", International Journal of Advanced Computer Science and Applications, vol.3, no.12, pp-76-80, 2012. (Journal citation)

[14] N.Sreenath and K.Muthuraj, "Optical Internet: Possible attacks on TCP/OBS networks", International Journal of Computer Science and Information Security, ISSN: 1947-5500, vol. 10, no. 12, pp- 20-24, December 2012. (Journal Citation)

[15] Guray Gurel, Onur Alparslan and Ezhan Karasan, " nOBS: an ns2 based simulation tool for performance evaluation of TCP traffic in OBS networks, " Annals of Telecommunications, vol. 62, no. 5-6, pp. 618-632, May 2007.


## BIOGRAPHIES

**Terrance Frederick Fernandez** received his M.Tech Degree in Distributed Computing Systems from Pondicherry Engineering College, India and B.Tech Degree in Computer Science and Engineering from Sri Manakula Vinayagar Engineering College *(affiliated to Pondicherry University)*, India. He qualified GATE with 92.53 percentile

**Brabagaran Karunanithi** doing M.Tech Degree in Information Security from Pondicherry Engineering College, Puducherry, India, received his B.Tech Degree in Information Technology from Trichy Engineering College, Trichy, India and diploma in Computer Engineering from Valivalam Desikar Polytechenic College, Nagapattinam, India.

**Sreenath Niladhurai** received his Ph.D Degree in Computer Science and Engineering from Indian Institute of Technology, Madras, Chennai, India, his M.Tech Degree from University of Hyderabad, India and his B.Tech in Electronics and Communication Engineering from Jawaharlal Nehru Technical University, Anathapur.