Secure Optical Internet: A Novel Attack Prevention Mechanism for an OBS node in TCP/OBS Networks

K. Muthuraj
Computer science and Engineering Department
Pondicherry Engineering College
Puducherry, India

N. Sreenath
Computer science and Engineering Department
Pondicherry Engineering College
Puducherry, India

***Abstract*—Optical Internet has become a strong development and its commercial use is growing rapidly. Due to transparency and virtual sharing infrastructure, they provide ultra-fast data rates with the help of optical burst switching technology, which transmits data in the form of bursts. From the security perspective, one of the OBS nodes in the optical network is compromised, causes the vulnerability. This paper is dealt to identify the vulnerabilities and named as burst hijacking attack and provide the prevention mechanism for the same. The NSFnet 14 nodes and the ns2 simulator with modified nOBS patch is used to simulate and verify the security parameters.**

Keywords-optical internet security; burst hijacking attack; threats and vulnerabilities in TCP/OBS networks.

I. INTRODUCTION

The benefits of optical internet have been known for quite awhile; but it was not until the invention of wavelength division multiplexing (WDM) that the potential of fiber was fully realized [1]. This divides the available bandwidth of the fiber into a number of separate wavelength channels and allows tens or hundreds of wavelength channels to be transmitted over a single optical fiber at a rate of 10 Gb/s/channel and beyond. This means that the data rate can reach 10 Tb/s in each individual fiber [2].

To carry IP traffic over WDM networks three switching technologies exist namely optical circuit switching (OCS), optical packet switching (OPS) and optical burst switching (OBS).Optical circuit switching, also known as lambda switching, can only switch at the wavelength level, and is not suitable for bursty internet traffic [3-5]. Optical packet switching, which can switch at the packet level with a fine granularity, is not practical in the foreseeable future. The two main obstacles are lack of random access optical buffers, and optical synchronization of the packet header and payload. Optical burst switching can provide fine granularity than optical circuit switching, and does not encounter the technical obstacles that optical packet switching faces. OBS is considered the most promising form of optical switching technology, which combines the advantages and avoids the shortcomings of OCS and OPS as tabulated in Table1 [6 -8].

OBS can provide a cost effective means of interconnecting heterogeneous networks regardless of lower-level protocols used in optical internet [9-11]. For example, an OBS network is able to transport 10 GB/s Ethernet traffic between two sub-networks without the need to interpret lower level protocols, or to make two geographically distant wireless networks to act as an integrated whole without protocol translations. The illustration of optical burst switching networks in the optical internet as shown in below Fig.1.

TABLE I. SCOPE OF SWITCHING TECHNOLOGY

Technique	Bandwidth	Latency	Buffer	Overhead	Adaptive
OCS	Low	High	-	Low	Low
OPS	High	Low	Yes	High	High
OBS	High	Low	-	Low	High

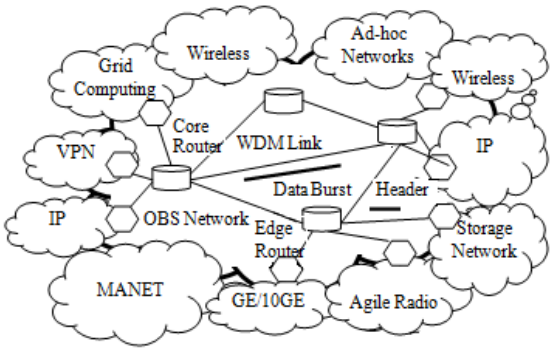

Figure 1. Illustration of optical burst switching network

In OBS networks, there is a strong separation between the control and data planes, which allows for great network manageability and flexibility. In addition, its dynamic nature leads to high network adaptability and scalability, which makes it quite suitable for transmission of bursty traffic. Unfortunately, OBS networks suffer from security vulnerabilities. Since every data burst is pass through the intermediate OBS routers. If one of the OBS intermediate routers is compromised, it causes security issues and denial of services [12-15].

The remainder of this paper is organized as follows. The architecture of OBS and about in-band and out-of-band signaling with its functional diagram is described in Section II. The Section III explains the TCP over OBS networks in Optical Internet. The Section IV demonstrates the main objective of this paper that is the identification of the attack on OBS node in TCP/OBS networks in Optical Internet as named as Burst hijacking attack. Section V depicts the attack

prevention mechanism for the same. The simulation results are shown in section VI. Finally we conclude and notify the future work in Section VII.

II. Optical Burst Switching Architecture

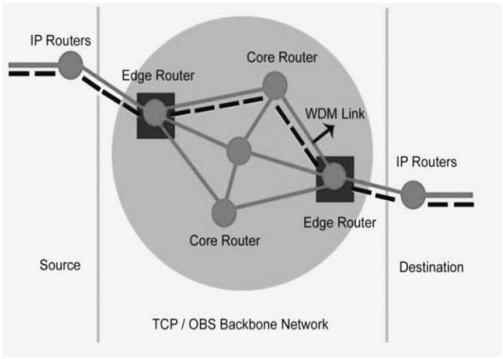

Figure 2. Architecture of optical burst switching

The pictorial representation of OBS architecture is shown in the above Fig. 2. In general, OBS network is composed of two types of routers, namely edge routers and core routers. Edge routers represent the electronic transit point between the burst-switched backbone and IP routers in an Optical Internet. The assembling of bursts from IP packets and disassembling of burst into IP packets is carried out at these edge routers. Core routers are connected to either edge routers or core routers. It transfers the incoming optical data into an outgoing link in the optical form without conversion of electronic form. In OBS, the basic switching entity is burst which contains the number of encapsulated packets. For every burst, there is a corresponding Burst Control Header (BCH) to establish a path from source to destination [16 -18]. BCH of a connection is sent prior to the transmission of Data Burst (DB) with specific offset time on the same wavelength channel is termed as In – band signaling shown in Fig. 3.

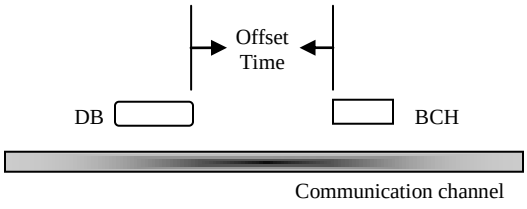

Figure 3. In – band signaling

All BCH's of various connections are sent on the same control channel and their corresponding DBs will sent on the different channels with specific offset time named as out – of – band signaling is shown in Fig. 4.

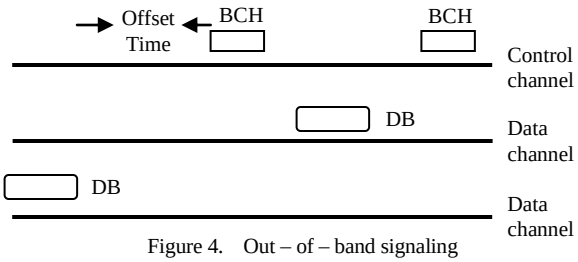

Figure 4. Out – of – band signaling

The Offset time is the transmission time gap between the BCH and DB, which is used to allow the control part in intermediate core nodes to reserve the required resources for the onward transmission of bursts.

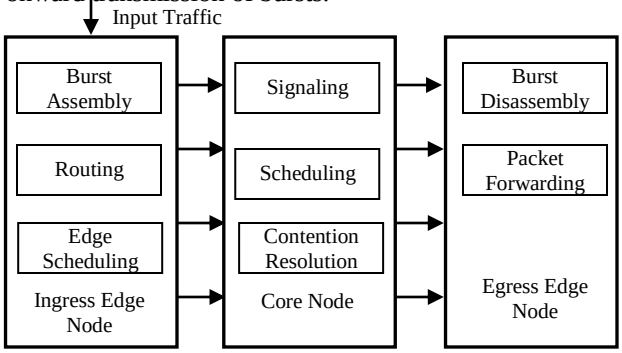

Figure 5. OBS functional diagram

The OBS functional diagram is shown in Fig. 5. It describes the ingress node is responsible for burst assembly, routing, wavelength assignment and scheduling of burst at the edge node. The core node is responsible for signaling and contention resolution. The egress edge node is responsible for disassembling the burst and forwarding the packets to the higher network layer [19-21].

III. TCP Over OBS Network

In a TCP/IP network, IP layer is involved in routing of packets, congestion control and addressing the nodes. When OBS is introduced in the network, it takes care of routing of data and congestion control. The routing information computed by IP layer need not be considered by OBS routers. It is because, the routes at the OBS are computed based on number of hops and wavelength availability. However, the addressing of the various nodes in the network is not taken care by OBS by default. Hence the functionality of IP may be limited to addressing and packet formation. Due to above reasons, this proposal consider the stack TCP/OBS rather than TCP/IP/OBS. This is shown in Fig. 6.

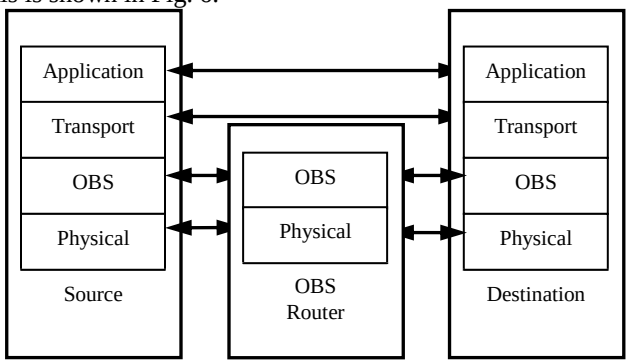

Figure 6. TCP/OBS Layer Architecture

IV. Burst Hijacking Attack

In Optical Internet, an optical virtual source node is inevitable for multicast routing, which is an optical node holds both wavelength splitting capability and wavelength conversion capability. It can transmit an incoming burst to multiple destinations on any wavelength. If it is compromised,

a new type of attack is possible named as burst hijacking attack. During the data transmission, Burst Control Header (BCH) is converted from an optical form to electronic form and is processed at every intermediate core node. The core node is to receive the BCH and setup the path for the corresponding Data Burst (DB) and forward to the next intermediate optical node until it reaches the egress node. If a compromised optical virtual source node receives, it can maliciously create a copy of original BCH and modifies its value to setup a path to a malicious destination then the corresponding DB will travel into the original destination as well as the malicious destination as shown in Fig. 7. The malicious destination will not send the acknowledgment for this hijacked burst and it escapes from being caught. Thus it compromises the authentication of data burst and also denial of service. This threat can be detected and named as Burst hijacking attack.

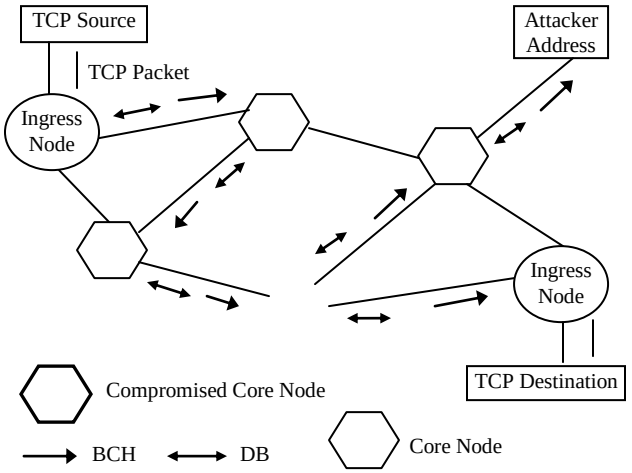

Figure 7. Burst hijacking attack

The provisioning of security has two aspects, attack detection and attack prevention. In attack detection the intermediate optical nodes are being monitored using trusted optical nodes. These trusted optical nodes use the statistical report to identify the malicious nodes. When an intermediate core router gets BCH, it collects the statistical information like burst id, source, destination, number of packets present inside the burst and the size of the burst. If the buffer is not present in the particular intermediate node then the collected statistical information is sent immediately to the trusted optical node. If it has buffers then it stores the statistical information and starts a timer. Once the timer gets expired or the buffer gets full, it sends the statistical information to the trusted optical node. The collected statistical information is stored in the buffer table of the trusted optical node based on the burst id. The statistical information is observed for some predetermined number of seconds and it should be analyzed and determines whether the node is behaving maliciously or not.

In Burst hijacking attack, a new connection established between the compromised intermediate virtual source node and destination node. Just to escape from being caught, the intelligent compromised virtual source node changes the burst id every time and creates a new connection between the intermediate core node and destination. In this case, the trusted optical node should check the burst size, number of packets inside the burst and detects the malicious optical node.

V. Attack Prevention Mechanism

recv (struct * PACKET packet)

{

Determine nodeType from packet.

if ((nodeType = ‘intermediate core node’)

OR

(nodeType = ‘egress node’))

{

a) Extract burst id, source, destination, num_of_packets, burst_size from the packet.

b) Create a new packet and store the extracted information inside the new packet.

c) Send the new packet to the trusted node

}

else if (nodeType == ‘trusted_node’)

{

a) Extract statistics from packet.

b) Insert the statistics into the linked list based on burst id.

c) Collect some more statistics.

d) Now extract the source, destination and burst id from the linked list head.

e) For burst hijacking attack, verify a new connection is established in virtual source node and burst_id or statistics matches with the original source and destination.

f) If the node’s trust value reaches below threshold, inform other nodes.

}

}

VI. Simulation Resesults

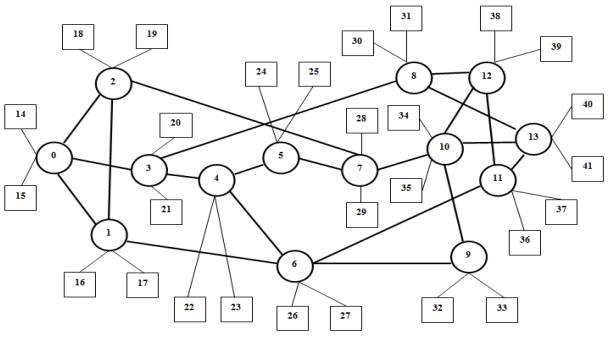

Figure 8. NSFNet topology with nodes 0 to 13

Topology	:	NSFNet
Number of Optical Nodes	:	14

Number of Electronic Nodes	:	28
Number of TCP/IP Connection	:	10
Max. Number of attacker nodes	:	03
Max. Number of packets	:	200
Max Lambda	:	20
Link Speed	:	1GB
Switch Time	:	0.000005

The simulations are done using nOBS, an ns2 based network simulator. NSFNet topology is used to demonstrate the effect of the BCH flooding attack as shown in Fig. 8. Nodes 0 to 13 represent the optical nodes and 14 to 41 represent the electronic nodes. The optical network is modeled with 1Gbps bandwidth and 10ms propagation delay. The TCP/IP links have 155 Mbps bandwidth each with 1 ms link propagation delay. In the beginning let us assume that there are no compromised nodes in the network. In that case, number of bursts sent by the ingress edge node is almost equal to number of bursts received by the egress edge node as shown in Fig. 9. Indicates that the number of bursts that are hijacked at that particular interval of time.

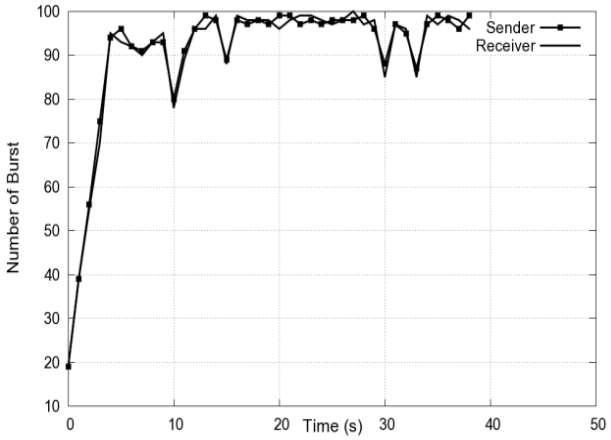

Figure 9. Number of bursts sent/received without any attacker nodes.

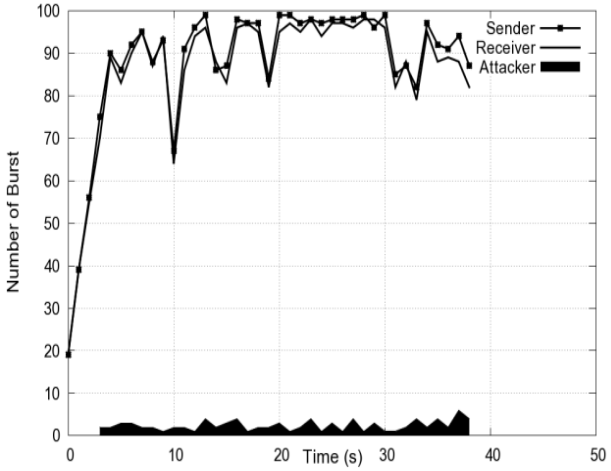

Figure 10. Effect of burst hijacking attack when the number of compromised node is 1.

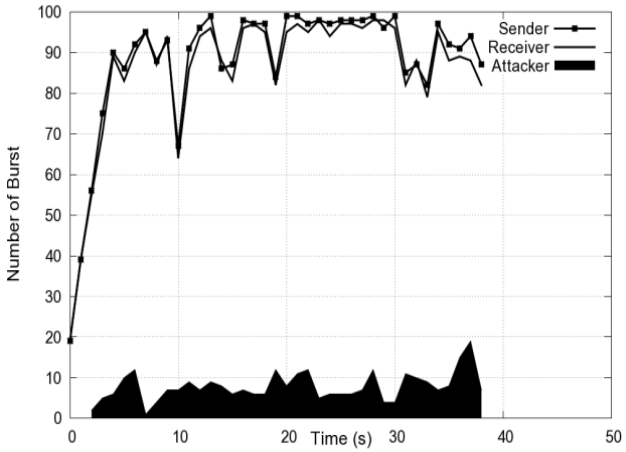

Figure 11. Effect of burst hijacking attack when the number of compromised node is 3.

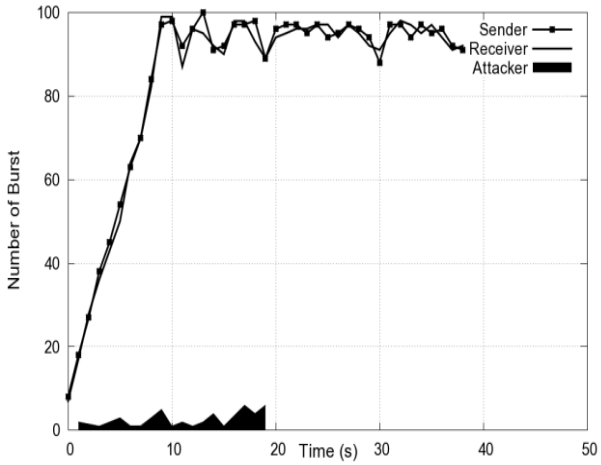

Figure 12. After implementing the solution to burst hijacking attack (number of compromised node = 1)

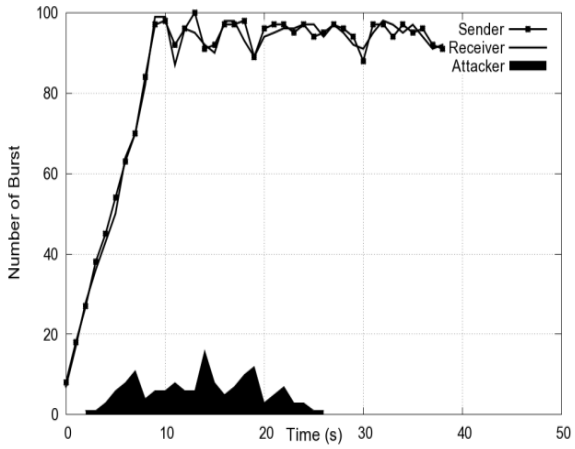

Figure 13. After implementing the solution to burst hijacking attack (number of compromised node = 3)

If the number of compromised nodes is 1 and 3 then the amount of hijacked bursts is also increased as shown in Fig. 10 and Fig. 11. And the Fig 12 and Fig. 13 shows the simulation results after implementing the solution for burst hijacking attack. Even though some bursts are hijacked initially, it is detected by the trusted nodes based on statistical information and an alternate trusted path is used for further communication. Thereby the burst hijacking attack is removed.

VII. Conclusion And Future Work

TCP/OBS networks are the future networks and optical burst switching will turn as the most broadly used technology in the mere future due to its speed and as it provides an end to end optical path among the communicating parties. Since optical burst switching has typical features, it is quite natural to suffer from the security attacks. In this paper, identified the new-fangled type of attack and named as Burst Hijacking Attack. From the statistical approach, its countermeasures are discussed from the normal scenario, attack scenario and attack removal scenario separately using ns2 simulator with the modified nOBS patch.

In the future when the optical burst switching is employed in everywhere then some more security attacks will arise. Future research in this area will help us to identify and remove other possible attack in TCP/OBS networks and make optical burst switching technique a superior one for optical internet.

Acknowledgment

The authors would like to thank the anonymous reviewers and the Editor – in – Chief for their valuable comments that have helped us to improve the manuscript.

References

[1] B. Mukherjee, “WDM Optical Communication Networks: Progress and Challenges,” IEEE Journal on Selected Areas in Communications, pp.1810-1823, October 2000.

[2] C. Qiao and M. Yoo, “Optical Burst Switching (OBS) - a New Paradigm for an Optical Internet”, Journal of High Speed Networks, pp.69-84, January 1999.

[3] S. Verma, H. Chaskar, and R. Ravikanth, “Optical Burst Switching: A Viable Solution for Terabit IP Backbone,” IEEE Network, pp. 48-53, November/December 2000.

[4] S. Yoo, S. J. B. Yoo, and B.Mukherjee, “All-Optical Packet Switching for Metropolitan Area Networks: Opportunities and Challenges,” IEEE Communications Magazine, vol. 39, pp. 142-148, March 2001.

[5] X. Cao, J. Li, Y. Chen, and C. Qiao, “Assembling TCP/IP Packets in Optical Burst Switched Networks., Proceeding of IEEE Globecom, December 2002.

[6] Guray Gurel and Ezhan Karasan, “Effect of Number of Burst Assemblies on TCP Performance in Optical Burst Switching Networks,” Proceedings of the IEEE BROADNETS, October 2006.

[7] M. Yoo and C. Qiao, “A Novel Switching Paradigm for Buffer-Less WDM Networks,” Optical Fiber Communication Conference (OFC), pp. 177-179, February 1999.

[8] J. P. Jue and V. M Vokkarane, “Optical Burst Switching,” Springer

[9] Science, 2005.

[10] M. Yoo and C. Qiao, “Choices, Features and Issues in Optical Burst Switching (OBS),” Optical Networking Magazine, vol. 1, pp. 36-44, April 1999.

[11] C. Siva Ram Murthy and Mohan Gurusamy, “WDM Optical Networks: Concepts, Design and Algorithms,” Prentice Hall PTR, November 2001.

[12] Pushpendra Kumar Chandra, Ashok Kumar Turuk, and Bibhudatta Sahoo, “Survey on Optical Burst Switching in WDM Networks,” Proceding of IEEE communications magazine, December 2009.

[13] Malathi Veeraraghavan and Tao Li, “Signaling Transport Options in GMPLS Networks: In-band or Out-of-band,” International Conference on Computer Communications and Networks, pp. 503-509, August, 2007.

[14] Yuhua Chen and Pramode K. Verma, “Secure Optical Burst Switching: Framework and Research Directions,” IEEE Communication Magazine, pp. 40-45, August 2008.

[15] Yuhua Chen, Pramode K. Verma, and Subhash Kak, “Embedded Security Framework for Integrated Classical and Quantum Cryptography Services in Optical Burst Switching Networks,” Security and Communication Networks, vol. 2, no. 6, pp. 546-554, November-December 2009.

[16] N. Sreenath, G. Mohan and C. Siva Ram Murthy, “Virtual Source Based Multicast Routing in WDM Optical Networks,” IEEE International Conference on Networks (ICON 2000), pp. 385-389, Singapore, September 2000.

[17] [16] 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-June 2007.

[18] J. Turner, “Terabit Burst Switching,” Journal of High Speed Networks, vol.8, pp. 3-16, January 1999.

[19] Turuk, A. K., Kumar, R., “A Novel Scheme to Reduce Burst-Loss and Provide QoS in Optical Burst switching Network, ” In proceeding of HiPC-2004, pp. 19-22, 2004.

[20] [19] Dolzer. K., Gauger C., Spath J., and Bodamer S.,” Evaluation of reservation mechanisms for optical burst switching ”, AEU International Journal of Electronics and Communications, vol. 55, no. 1, pp. 18-26 April 2001.

[21] Siva Subramanian, P., Muthuraj K.,” Threats in Optical Burst Switched Network. Int. J.Comp. Tech. Appl. “, vol. 2, no. 3, pp. 510-514, July 2011.

[22] N. Sreenath, K. Muthuraj, and P. Sivasubramanian , “ Secure Optical Internet:Attack Detection and Prevention Mechanism,’’ International Conference on Computing, Electronics and Electrical Technologies, 2012.

AUTHORS PROFILE

K. Muthuraj is a Research Scholar and pursuing a Doctoral Degree in Computer science and Engineering at the Department of Computer science and Engineering at Pondicherry Engineering College, Pillaichavady, Puducherry – 605014, India. He received his B.E in Computer science and Engineering (2000) from Madurai Kamaraj University, Madurai, Tamilnadu, India. He received his M.E in Computer science and Engineering (2008) from Anna University, Chennai, Tamilnadu. His research areas are high speed networks and Optical Internet..

Dr. N. Sreenath is a professor and Head of the Department of Computer science and Engineering at Pondicherry Engineering College, Pillaichavady, Puducherry – 605014, India. He received his B.Tech in Electronics and Communication Engineering (1987) from JNTU College of Engineering, Ananthapur – 515002, Andra Pradesh, India. He received his M.Tech in Computer science and Engineering (1990) from University of Hyderabad, India. He received his Ph.D in Computer science and Engineering (2003) from IIT Madras. His research areas are high speed networks and Optical networks.