Optical Internet Security: A new Time based threat identification and its prevention

K. Muthuraj¹ and N. Sreenath²
¹Research Scholar, ²Professor, Department of Computer science and Engineering
Pondicherry Engineering College, Puducherry, India
muthuraj@pec.edu, nsreenath@pec.edu

ABSTRACT

Optical Internet (OI), which are driving the demand for increased transmission rates and bandwidth–hungry applications and its services using dedicated optical routers. To cater this huge bandwidth demand, Transmission Control Protocol (TCP) is the prevailing mechanism and OBS (Optical Burst Switching) is the rapid technology for support this Optical Internet traffic. Due to the sensitivity of relying role in Optical Internet, security becomes a major concern in optical networks. In this paper, describes that the Optical Internet suffers from the newfangled denial of service vulnerability and it is named as time out attack in Optical Internet and the prevention mechanism for the same is also provided. The ns2 simulator with modified nOBS patch is used to simulate and verify the security parameters.

Key words- optical internet security, time out attack, threats and vulnerabilities in TCP over OBS networks, secure optical burst switching, attacks on optical networks.

I. INTRODUCTION

The exponential growth of bandwidth demand is driving the need for routers that operate at increasing bit rates and that have a very large number of ports. To meet this growing demand, routers that scale with the demand on both the bit-rate and port-count are needed. The increasing demand for bandwidth has led to the development of optical fibers that could support very high bit-rates. This can be achieved through Time division Multiplexing (TDM), Code Division Multiplexing (CDM) and Wavelength Division Multiplexing (WDM). CDM chip rate and TDM bit rate are very high when compared to the electronic processing speed of an end user’s network interface.

Therefore WDM is more attractive than CDM and TDM because of no such requirements. For long haul communication, WDM is the current favorite multiplexing technology in optical communication networks and Wavelength Division Multiplexing is the preferred solution for providing higher bandwidth; WDM increases the bandwidth of a single optical fiber by creating multiple virtual fibers, each carrying multi-gigabits of traffic per second, on a single fiber. The demand for more bandwidth is fueled by packet switched IP traffic and the traffic generated by higher layer protocols and applications, such as the World Wide Web which is bursty in nature shown in below Fig 1 [1-5].

Recently, Optical Burst Switching (OBS) was developed as an alternative networking technology [6], which represents a balance between Optical Circuit Switching (OCS) and Optical Packet Switching (OPS). In OCS, one or more wavelengths are reserved between source and destination, relatively simple to realize but requiring a certain amount of time for channel establishment and release. Furthermore, each channel occupies atleast a full wavelength (2,5 or 10 Gb/s), which is very inefficient when the network has to transport variable traffic, like the dominant IP protocol. This dominance of IP and its variability strongly motivates the development of OPS, where packets are entirely switched in the optical domain. The lack of efficient optical storage capacity and the limited optical processing functionalities, however,
hinder cost-effective implementation of OPS in the foreseeable future. OBS tries to combine the best features of both OCS and OPS, while avoiding the aforementioned drawbacks. In [7], the main characteristics of OBS were defined as:

- OBS granularity is between OCS and OPS.
- Separation between burst control header and data burst. Header and payload are usually carried on different channels with a strong separation in time.
- Resources are allocated without explicit two-way end-to-end signalling, instead so-called one-pass reservation is applied.
- Bursts may have variable lengths.
- Burst switching does not require buffering.

OBS can provide a cost effective means of interconnecting heterogeneous networks regardless of lower-level protocols used in OI. 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 [8-9].

The remainder of this paper is organized as follows. The architecture of Optical burst switching is described in Section II. The Section III demonstrates the main objective of this paper that is, the new time based vulnerability named as TIMEOUT attack on an OBS node in Optical Internet detection and the prevention mechanism for the same. Section IV depicts the simulation using NSFnet 14 node topology and results are plotted with the help of GNUplot. Finally we conclude and notify the future work in Section V.

II. ARCHITECTURE OF OPTICAL BURST SWITCHING

Optical burst switching (OBS) is the next generation Optical Internet with TCP over WDM as the core architecture and the pictorial representation are shown in below Fig. 2.

In OBS, two types of routers exist namely Edge routers and Core routers. Ingress Edge routers are responsible for assembling the IP packets into burst, scheduling, routing and wavelength assignment. Egress Edge routers are responsible for disassembling the burst into IP packets and packet forwarding. Core routers are responsible for scheduling, signaling and contention resolution. The functional diagram is given in the below Table 1 [10-14].

<table>
<thead>
<tr>
<th>Ingress Edge Router</th>
<th>Core Router</th>
<th>Egress Edge Router</th>
</tr>
</thead>
<tbody>
<tr>
<td>Burst Assembly</td>
<td>Signaling</td>
<td>Burst Disassembly</td>
</tr>
<tr>
<td>Wavelength Assignment</td>
<td>Scheduling</td>
<td>Packet Forwarding</td>
</tr>
<tr>
<td>Edge scheduling</td>
<td>Contention Resolution</td>
<td></td>
</tr>
</tbody>
</table>

Table 1 – OBS Funcional Diagram

And the basic switching entity in OBS 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. BCH of a connection is sent prior to the transmission of Data Burst (DB) to specific offset time on the same wavelength channel is termed as an 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. 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 [15 -16].

There are two kinds of burst assembling process is done, named as timer and threshold based. In timer based approach, a timer will be started on the source ingress node. All the IP packets which are collected and reach the same destination are formed as data burst. Once the timer gets expired, a burst control header will be generated and sent ahead of data burst. In threshold based, a burst is created and sent into the optical burst switched network when the total size of the IP packets reaches a threshold value. The wavelength reservation scheme is followed to reserve the wavelength for data burst. The three popular wavelength reservation methods are tell and go, just in time and just enough time. In tell and go method, data burst will be after the burst control header with a small
offset time. Just in time is a direct reservation method. Here, nodes reserve the resources as soon as the control signal processing gets over. Just enough time is a delayed reservation method. Here, the size of data burst is decided before the control signal is transmitted by the source. The offset between the control signal and data burst is also calculated based on the hop count between source and destination [17].

In an IP network, the IP layer is involved in the routing of packets, congestion control and addressing the nodes. When OBS is introduced into 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 does not take care by OBS by default. Hence the functionality of IP may be limited to addressing and packet formation. Due to above reasons, this proposal considers the stack TCP over OBS rather than TCP/IP/OBS [18 – 19].

III. TIMEOUT ATTACK DETECTION AND PREVENTION MECHANISM

In TCP over OBS networks in Optical Internet, the ingress router the packets are assembled to form a burst. There are mainly two assembling schemes as described in the above section. First is based on the threshold based and the second is based on the timer-based. In a timer based scheme, a timer is started at the initialization of burst assembly. The latter is based on the maximum number of packets. A data burst is generated when the timer exceeds the burst assembly period or when the maximum number of packets is reached. Here in this attack the TIMEOUT value of optical nodes of TCP over OBS Network is changed to a very low value. As a result ingress node starts to produce many small bursts and send to the destination causing unwanted traffic. This is shown in below Fig. 3.

The solution for this attack just converts the value of the burst formation to standard value it gets changed by the attacker. So, standard value for the burst formation in both schemes should be stored in the ingress node. The node creates the burst as per the value stored in it. The attack can be implemented whenever an attacker compromises the ingress node and changes the standard value of very low value. So, this attack will get implemented by creation of very small burst. The solution can be given by there should be a procedure which investigates the standard value after creation of the burst.

This new procedure can be incurred in the ingress node. By invoking this procedure which checks the current value of the TIMEOUT with the standard value of the TIMEOUT, that is to identified by running the nOBS with the modified patch for different TIMEOUT & MAX_NUM_PACKET values of optical node. If the current value of the TIMEOUT and the standard TIMEOUT value will be vary then the standard TIMEOUT value is assigned to the current TIMEOUT value. This may treated as the countermeasure for the same.

IV. SIMULATION RESULTS

Simulation is one of the important technologies in modern time. Simulation depicts the actual network by means of software. The simulation is very economical because it can carry out experiments without actual hardware. There are many numbers of network simulators are available. There are many numbers of network simulators are available. This proposed attack in TCP over OBS network in Optical Internet is done using the ns-2 simulator with a modified nOBS patch which is called as nOBS [20 - 23].

<table>
<thead>
<tr>
<th>Topology</th>
<th>NSFNet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Optical Nodes</td>
<td>14</td>
</tr>
<tr>
<td>Number of Electronic Nodes</td>
<td>28</td>
</tr>
<tr>
<td>Number of TCP/IP Connection</td>
<td>10</td>
</tr>
<tr>
<td>Max. Number of attacker nodes</td>
<td>03</td>
</tr>
<tr>
<td>Max. Number of packets</td>
<td>200</td>
</tr>
<tr>
<td>Max Lambda</td>
<td>20</td>
</tr>
<tr>
<td>Link Speed</td>
<td>1GB</td>
</tr>
<tr>
<td>Switch Time</td>
<td>0.000005</td>
</tr>
</tbody>
</table>

The topology creation details of the proposed simulation as follows, Optical nodes are numbered from nodes 0 to nodes 13 and 14 to 41 behaves as the electronic nodes. The optical network is posed with 1000Mb bandwidth and 10ms propagation delay. The TCP/IP links posses 155Mbps bandwidth each with 1ms link propagation delay described in above. The NSFNet topology is employed to delineate the aftermath of the TIMEOUT attack in the ingress node of the TCP / OBS network as exhibited in the below Fig. 4.

Fig 3 - Time out attack detection mechanism
In OBS, Timeout attack can be identified by using the nOBS patch in ingress node. As discussed in the earlier section the burstification process of packets in the ingress edge router is based on either timeout or maximum numbers of packets allowed. In nOBS patch the burstification process is based on both the timeout and maximum number of packets allowed.

The value of the TIMEOUT and MAX_PACKET_NUM is predefined in the patch. If an attacker injects a code to the nOBS patch that modifies the value of the TIMEOUT resulting in the formation of the burst which is smaller in size. Since the bursts are smaller in size number of bursts are generated during attack leading to disrupted traffic. In our simulation we triggered the attack at 10 ms and the solution is provided at 20 ms.

The below plotted GNUplot graph shows the formation of burst with the stipulated time. The number of burst formation before the attack is also plotted. This normal scenario of burst formation is shown in the below Fig. 5. Time is taken in the X-axis where as the number of bursts formed is taken in the Y-axis.

The attack is identified in the below Fig. 6. Number of bursts formed is taken in the Y-axis and time taken in the X-axis. Attack is triggered at 10ms producing many small bursts with respect to time.

Below in Fig. 7 shows the solution triggered at 20 ms. Procedure is called to change the TIME_OUT value to Standard value. Thus, the solution gets implemented. Y-axis shows the number of bursts formed and X-axis shows the time. Number of bursts formed gets changed to default value when changing the TIME_OUT value of Standard value. Thus, ingress node starts producing the actual number of bursts.

![Fig 4- NSFNet topology with nodes 0 to 13](image)

![Fig 5 - Number of Bursts generated vs Time before attack](image)

![Fig 6 - Number of Bursts generated vs Time after the attack is triggered at 10ms](image)

![Fig 7 - Number of Bursts generated vs Time after the solution is triggered at 20ms](image)
V. CONCLUSION AND FUTURE WORK

Optical Internet is the future internet which using TCP over OBS networks are the backbone 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 vulnerabilities. In this paper we identified the newfangled type of based attack and it’s named as TIMEOUT attack and provides a prevention mechanism for the same using ns2 simulator with the modified nOBS patch and the results are plotted using Gnuplot.

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

VI. 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.

VII. REFERENCES


[22] Mohammed A.Al-Shargabi, Abdul Samad Ismail, Sevia


VIII. AUTHORS

**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.