CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

Communication networks are necessary in modern society. Their role is to transmit/receive information quickly and reliably. A communication network is built of nodes that process information, and provide links between the nodes that transport the information. Telecommunication networks carry information throughout parts, which are geographically far apart. An information source can be a computer, a human being, a teleprompter, a data terminal and so on. These sources exchange information, which may in the form of a telephone conversation or a file transfer between two computers or message transfer between two terminals etc. Today it is almost true to state that telecommunication systems are the symbol of our information age. With the rapidly increasing traffic and undefined growth of cyberspace, communication has become an integral part of our life. The future challenges are enormous with expectation of a rapid growth in terms of new services and number of users (Turner 1999, Verma et al. 2000).

A modern society therefore needs new facilities including very high bandwidth switched data networks, a large communication satellite with small and cheap earth antennas. The beginning of the new era required many advancements due to the global popularity of the Internet. The role of Internet is increasing exponentially during the late 1990s. With this dramatic increase of Internet users the need for the network with lower cost, large bandwidth
and efficiency was required. Therefore there was a continuous demand for networks of high capacity at low cost. During this period as a supporting hand optical data communication was recognized (Chlamtac et al. 1992).

Optical networks provide higher capacity and reduced costs for new applications such as the video, Internet, multimedia technology and advanced digital services. Since its invention in the early 1970s the demand and the craze for optical fibers has reached the zenith. The uses of optical fiber today are quite numerous. With the explosion of information traffic due to the Internet, the need for a transmission medium with bandwidth capabilities for handling such vast volume of information is paramount. Fiber optics, with its comparatively infinite bandwidth, has proved to be the solution. Transporting a huge volume of data requires high reliability and consistency in performance. Simplicity of maintenance and low operational cost has been widely considered as the key factors in expansion of optical networks (Kelly 2003, Weichenberg et al. 2009). In addition, upgrade-ability within a reasonable cost and robustness, remain to be critical issues in turning optical technology into the viable solution for future requirements.

The optical networks have replaced copper cables with optical fibers as the medium of transmission. These networks are capable of using multiple carrier wavelengths that are multiplexed onto a single fiber thus offering an increase in bandwidth. This technique is depicted as Wavelength Division Multiplexing (WDM). WDM takes optical signals and converts them to a specific wavelength or frequency, and then sends them on the same fiber. There is a growing interest in deploying wavelength division multiplexed systems to meet the high bandwidth needs of Internet traffic, especially for global Internet Service Providers (ISPs) (Mohan et al. 2005). WDM is a point-to-point transmission technology, in its simplest form that allows a service provider to increase the transmission bandwidth of a fiber with dense
WDM (DWDM) multiplexers/demultiplexers. When reconfigurability is added to WDM multiplexers/demultiplexers, even the light paths can be reconfigured, when needed (Lamba & Kumar 2012).

The role of WDM technology has been extended from a simple point-to-point transmission technology to a networking technology. Each piece of equipment which sends an optical signal has an illusion that it has its own fiber. It gets more data to travel not by increasing speed but allowing them to travel in own parallel dedicated lines. Each line travels at different speeds and each of them is independent WDM network elements, such as Optical Add/Drop Multiplexers (OADMs) and Optical Cross Connects (OXC), which are already in use. Optical cross connects, also referred to as wavelength routers, which may or may not have wavelength translation capability. Most current networks employ electronic processing and use the optical fiber only as a transmission medium. The function of switching and processing of data is performed by converting an optical signal back to electronic form (Mukherjee 2000). Switching technologies are required for carrying IP traffic over WDM network.

### 1.2 SWITCHING PARADIGMS

A switch is a word with two different meanings. A brief definition is that, a switch is a device which is used for switching signals from input ports to output ports (Ramaswami & Sivarajan 2001). However, a switch can also mean a simple device with a few components. It can also be a complex device that consists of blocks with complex controls, delay line buffers, wavelength converters and simple switches. Furthermore, a switch can also mean to be a component and an entire node in a network.
The optical switching types are classified as follows:

1. Optical Circuit Switching
2. Optical Packet Switching
3. Optical Burst Switching

### 1.2.1 Optical Circuit Switching

In circuit switching, a dedicated path is established for communication. E.g. Telephone networks. A switching node can simply provide a transmission path between other switches and it may not be connected to any terminal. Depending on the transmission technology and the physical transmission media, a switching node can be either optical or electrical based. In Optical Circuit Switching (OCS), a dedicated path is established between two nodes before any data transmission takes place. The dedicated path referred to here is assignment of a specific wavelength to each source destination pair. One of the major advantages of circuit switching is that it is essentially a transparent service where no storage is needed. Once the connection is established, constant-rate of data is transported between the connected nodes (Christophgaugher et al. 2001).

In an optical network, transmission media, viz., WDM links and switching nodes are optical. With the help of WDM technology, optical transmission is structured into a number of over-lapping bands of wavelength. Each communication channel can be supported by only a single wavelength. The main objective of this switching method is to assign a specific wavelength to each source to a destination pair which is shown in Figure 1.1. OCS handles a huge volume of long lived data transfer. The optical transmission spectrum is divided into a number of over-lapping wavelength bands by using the transmission technology. Each communication channel is
supported by a single wavelength that operates at the peak electronic rate. Circuit-switching technology has also major jump outs which make it less popular for certain applications. An important consequence of circuit switching is that all the resources should be available and dedicated through the network between terminals before the communication takes place. Or else the communication request will be blocked, thus resulting in potential channel in efficiency. But a well-established data path is required before starting transmission. Since this technique is a virtual point to point link, when N nodes are used, the requirement of wavelength is $O(N^2)$ which is practically impossible (Xiong et al. 2000). So the difficulty to support variable data rates as the traffic increases means longer time for setting up a circuit.

![Optical circuit switching](image)

**Figure 1.1 Optical circuit switching**

High utilization is required for voice communications. This can be achieved as the idle time is small. Another major issue with circuit switching is that in order to setup circuits between end-stations, circuit switching facilities must be capable of processing large number of signalling at high-speed. Hence, existing systems may not be efficient for bursty traffic with
short message durations and sporadic transmissions. The main disadvantage lies in the non scalability of this technique since \( O \left( N^2 \right) \) wavelengths are required for \( N \) nodes due to virtual point to point link. Moreover, it does not adapt to the variations in the traffic matrix. OCS requires a certain amount of time for channel establishment and the release is independent of the connection holding time. This circuit switching concept has been replaced by a competitor such as packet switching. This is an alternate approach to overcome the pitfalls in optical circuit switching.

### 1.2.2 Optical Packet Switching

With the development of various technologies in the Internet traffic during the past decades, circuit switching seems to have lost its importance. This circuit switching concept has been replaced by alternatives such as packet switching. This is an alternative paradigm to overcome the pitfalls in optical circuit switching. Here, a long message is divided into pieces called packets. Each packet contains a header. Optical packet networks are those where the switching operations are performed optically (Qiao et al. 2006). In Optical Packet Switching (OPS) the payload is switched on optically. Optical Packet Switching can be faster, and also cheaper to purchase and maintain than traditional switching with the Optical/Electrical/Optical (O/E/O) conversion. OPS hardware will consume less power, dissipate less heat and occupy less space compared to electronic equipment. This is the important feature which makes OPS more popular than the electronic equipment. In optical networks, the components and the networks themselves have developed rapidly. However, there are still many unsolved questions. Now many networks are all-optical circuit switched networks, but all of them are still in the early stage of development, though developing fast (Yoo et al. 2001).
The main problem is the infancy of optical devices, especially the lack of optical random access memory. Moreover, adaptation to ultra-switching requirement is also not possible. The packets are limited due to buffering capacity at each node. The reason for this is the use of store and forward technique. The links are occupied on the basis of the demand alone. The emerging version of optical packet switching is photonic slot routing which is defined as the process of switching packets on different wavelength simultaneously. An OPS is distinguished as synchronous and asynchronous. Synchronous method is based on the time domain. Hence the division of time domain into slots takes place, during which packets are sent and received, while in the asynchronous method, packets arrive at any time instant, the time domain is slotted. Depending upon the header packet processing technology, optical packet switching can be divided into transparent OPS and all optical packet switching. When the packet header is processed electronically, this version of OPS is called transparent OPS.

Similarly when the packet headers are processed optically, this version of OPS is called all-optical packet switching. The corresponding data payload waits in the fiber line until completion of the conversion process and then they are forwarded to the next node. In the switching node, the wavelength is dynamically time shared with a limited number of available wavelengths. Here the links are occupied depending upon the demand. When there is any congestion, an alternate route will be provided (Chlamtac & Fumagalli 1996). The development of wavelength division multiplexing opens up a new horizon in optical networks and promises to be one of the best solutions for the high demand of the bandwidth. But still with this advanced technology, many problems fills out, especially those relating to the architecture to be used in optical networks so as to take advantage of the huge potential of this technique. Many approaches and architectures have been proposed in literatures to carry information in optical domain.
1.2.3 Optical Burst Switching

Introduction of a new paradigm, which combines both the advantages of optical circuit switching and optical packet switching is the optical burst switching. Due to technological constraints, optical burst switching has only been initiated. Circuit and packet switching have been used for many years for voice and data communications. The added advantage of optical burst switching seems to be better than optical packet switching since data burst does not need to be buffered or processed at intermediate nodes (Chen et al. 2004). The comparison of optical burst switching with optical circuit and packet switching are shown in Table 1.1.

Table 1.1 Feature comparisons between various switching paradigms

<table>
<thead>
<tr>
<th>Technique</th>
<th>Bandwidth</th>
<th>Latency</th>
<th>Buffering</th>
<th>Overhead</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCS</td>
<td>Low</td>
<td>High</td>
<td>No</td>
<td>Low</td>
</tr>
<tr>
<td>OPS</td>
<td>High</td>
<td>Low</td>
<td>Yes</td>
<td>High</td>
</tr>
<tr>
<td>OBS</td>
<td>High</td>
<td>Low</td>
<td>Yes</td>
<td>Low</td>
</tr>
</tbody>
</table>

OBS provides a cost effective means of interconnecting heterogeneous networks regardless of the lower-level protocols used in these networks (Biaz & Vaidya 2005). OBS requires limited delay of the data at intermediate nodes as in OCS, and ensures efficient bandwidth utilization on a fiber link just as in OPS. This allows the strengths of optical switching technologies to be leveraged effectively and the problem of buffering in the optical domain is circumvented. There is a separation between header and data. Header and data are usually carried in different channels with a strong separation in time called offset (Qiao & Yoo 2000, Barakat & Sargent 2004).
An optical burst switched network is composed of OBS nodes that are interconnected via optical network. The OBS network architecture is shown in Figure 1.2. This network has two types of routers, namely, the edge router and the core router (Haselton 1983). Edge nodes are at the interface between the electronic and the optical domains. Edge router can be as ingress or egress node. The ingress node is responsible for burst assembly, routing, wavelength assignment, scheduling of burst at edge node. Packets are assembled into bursts at ingress edge node, which are then routed through the OBS network. The egress edge node is responsible for disassembling the burst. The core node is responsible for signalling, scheduling, resolving contention (Battestilli & Perros 2003).

An optical burst consists of two parts, viz., a header and a data burst. The header is called the Control Packet (CP) and is transmitted separately from the data. In OBS, a burst is the basic characteristic feature of this data. Burst is a variable length data packet, assembled at an ingress router by aggregating a number of various inputs, which may be received from a single host or from multiple hosts belonging to the same or different access networks. Bursts may have variable sizes. In general, the range of the burst can be from 40,000 to 1, 20,000 packets. This process of aggregating several
packets into a burst is called burst assembly. During burst assembly, data is buffered at the edge node where electronic RAM is easily available. Data bursts are disassembled at the egress router into packets.

A control packet is transmitted over a separate control channel before each data burst is transmitted. The control packet contains information about the sender, receiver and transmission wavelength of the corresponding burst. This control packet, which is sent ahead of the data burst, undergoes O/E/O conversion and is processed electronically at each intermediate node. This process is called as burst resource reservation (Eric et al. 2009).

OBS is a two way reservation scheme, wherein a control packet is sent prior to the burst to reserve the resources. The data burst is sent after a certain offset time. Offset time is the transmission time gap between burst control packet and data burst, which is used for reserving the required resources for the onward transmission of bursts. Resources are allocated without explicit two-way end to-end signalling. Instead, the so-called one-pass reservation is applied (Gauger et al. 2004). The important parameters that govern the OBS network are the burst managers which focus on the maximum burst size, offset time and the burst timeout. Buffering is not required in OBS.

1.2.3.1 Burst assembly algorithm

Burst generation and assembly define how packets are assembled to form an optical burst. The burst assembly process starts with the arrival of a packet from a high layer application and continues until a predefined criterion is met. The optical burst consists of an integral number of variable size packets. In general, each edge router maintains a separate (virtual) queue for each destination node to hold the data packets. Each queue is handled by a
separate burst assembler, while a single link scheduler is commissioned to assign wavelengths and schedule bursts for transmission (Luo et al. 2003).

The burst assembly criterion indicates the formation of a new burst when the actual process of gathering packets stops. This criterion is of paramount importance for the network, since it affects traffic characteristics such as burst size, burst inter-arrival times as well as the packet delay. The packet delay is defined as the time that the packets should wait for before burst transmission. The typical burst assembly module is shown in Figure 1.3.

**Figure 1.3 Burst assembly module**

All incoming packets are forwarded to the corresponding queue according to their destinations. When the queue size reaches a threshold, the packets in this queue are sent out as a burst. The choice of burst assembly algorithms depends on the type of traffic being transmitted.

The assembly algorithms are classified as Fixed Assembly Period Algorithms (FAP) and Dynamic Assembly Period Algorithms (DAP).

Fixed Assembly Period Algorithms (FAP) can again be classified into three types:
1. Time-based fixed assembly period (Time-FAP) algorithm
2. Threshold-based FAP Algorithm
3. Minimum Burst length Maximum Assembly Period algorithm (MBMAP)

In this Time-based fixed assembly period (Time-FAP) algorithm, the bursts are assembled and sent into the assembly timers with periodic time intervals. The bursts with different destinations and QoS parameters are assembled according to the different assembly timers (Praveen et al. 2006). Problem in Time-FAP algorithm is the variation in burst length as the traffic load intensity changes.

Timer-based algorithms are suitable for time-constrained traffic such as real-time applications considering the upper bound of the burst assembly delay is limited. In a time based scheme, a timer is started at the initiation of burst assembly. As for Time based Algorithms, the entire algorithm is based on assembly time period. When the assembly period is too large, the packet delay is also too large at the edge node, being intolerable. Likewise when the assembly period is too small, too many small bursts are being generated it results in a higher control overhead (Zhou et al. 2004).

In the threshold-based FAP Algorithm, a fixed burst length is chosen as the assembly parameter. When the burst length exceeds the initialized threshold, the packets in the burstifier are assembled together as a burst. The problem associated with this technique is that network delay gets increased when the traffic load in the network is low. The shortcoming of the threshold-based scheme is that it does not provide any guarantee on the assembly delay that packets will experience. For a time-insensitive application such as file transmission, a threshold based scheme may be more
appropriate for reduction of the overhead of the control packets and increase in OBS transmission efficiency (Zhu et al. 2005).

The Minimum Burst length Maximum Assembly Period algorithm (MBMAP) uses two parameters for assembly of bursts namely minimum burst length (MBL) and maximum assembly period (MAP). When the burst length reaches MBL before MAP expires, the burst is assembled. Otherwise, it should wait for the timeout. When the traffic load is low, MBMAP algorithm avoids the meaningless waiting delay.

The previous burst length and the current burst length are the two states at the edge node in DAP algorithm. According to the rule of the slow start, the algorithm is initialized in such a way that the minimum burst contains only one Transmission Control Protocol (TCP) segment. The assembly period for the next burst is predicted as \( T_b = \text{current burst length}/B*2 \). When the burst is assembled as per the predicted assembly period, its burst length remains the current burst length, compared with the previous burst length. The comparison of two burst lengths predicts the current state of TCP window and the assembly period for the next assembly is updated and is defined as Dynamic assembly algorithm.

1.2.3.2 Reservation algorithm

Just Enough Time (JET) protocol is used in the optical burst switching, for sending a packet from origin node to delivery node and comes under the delayed reservation scheme. It is meant for Two-way reservation protocol and has some unique characteristics such as delayed reservation (DR) and the ability of combining delayed reservation with the help of fiber delay lines (FDL) based buffered burst multiplexers (BBM) (Liu & Liu 2002). In the late eighties, the Tell And Go (TAG) protocol was used for optical burst switching. It lacks these features of JET protocol as it is a one way
reservation mechanism. At first, the protocol JET helps the source node to send the control packet through the physical/static links between the IP entities. In order to maintain the routing table, topology (structure of the network) and the information about the source node and destination node; packet switching supports the JET protocol between the contiguous IP entities. The control packet reserves the path for the burst to reach the destination based on the Internet protocol (IP) addresses of the links by composing all the optical switches along their path (Dolzer et al. 2001).

This way the JET protocol supports the optical burst switching by depreciating the latency and the processing load in the IP layer. Once the burst passes through the particular link, the wavelength used by the burst gets released automatically or by an explicit mode. Due to this feature, the burst can reserve the bandwidth of the similar wavelength on a particular link from different source to different destination node. When a control packet fails to set aside a bandwidth for the burst in any node, the burst gets blocked or dropped from in a specific node. So, the negative response is sent to the related source node for retransmission. The optical burst switching supports both reliable and non-reliable transmissions between the IP entities (Shihada & Ho 2008). The action of retransmission is necessary for both the control packet and the burst from source node to destination node. The OBS should have some applications protocols for the retransmission action (Vokkarane & Jue 2003).

Sometimes the OBS sends data automatically to the destination node with the help of an upper application layer protocol like TCP. Some wastage of bandwidth takes place due to this retransmission. In order to avoid this, the blocked burst should be stored in an electronic buffer after the two conversions takes place (Hsu et al. 2002). They are optical to electronic conversion and electronic to optical conversion based on the respective
destination. The use of fiber delay lines in OBS is to create delays at intermediate nodes. It is not mandatory but it support OBS to eliminate the bandwidth waste and accelerate the performance of quality of service in the network (Vokkarane et al. 2002).

The protocol used in the optical burst switching and coming under the immediate reservation scheme is known as Just In Time (JIT). The source node sends the control burst for wavelength reservation to the upcoming data burst. Once the wavelength is set aside or utilized, the control burst processing is over in the network. The data burst from the source node is transported to the intended delivery address over the path of the control burst. It takes place when the transportation of the burst after some delay (Offset time) and should be greater than the control burst’s processing time in the network (Barakat & Saragent2004). When the control burst reaches closer to the destination node, the offset time decreases and the idle time of the reserved wavelength also decreases.

It means the data burst in the particular path getting transmitted after some time. It has some difference in features and characteristics between them. There is time gap or time line in JIT between the control and data burst due to which buffering is avoided at each node and wavelength is reserved until the first bit of the data burst arrives at each Optical Burst Switching using JIT protocol and every node in the link. The reserved wavelength will be released after the data burst passes through the link by using the in-band terminator.

1.3 ATTACKS AND SECURITY VULNERABILITIES IN OBS NETWORKS

OBS proves to be a better technology to tackle the huge bandwidth constraints. Unfortunately, OBS networks suffer from security vulnerability.
Although IP sec can be used to secure IP networks, OBS networks can provide security services to traffic that do not necessarily have an IP layer. The control and data signal are sent separately. The control signal is to be converted into electronic form. During this conversion process there is a possibility of an intermediate node to change the contents of control signal, leading to security issues. Certain parameters have to be satisfied to ensure better data transfer taking place. This is a challenging problem in optical domain. OBS networks show great promise in providing cost effective interconnection solutions to the ever growing Internet. When any operation is performed in an OBS network, while maintaining the security principles it is called the normal behaviour of a network. First and the foremost feature is secrecy (Yuhuachen et al. 2008).

Only the ingress and intended egress node should be able to understand the contents of the transmitted message. As the eavesdroppers may intercept the message, the message should be encrypted so that an intercepted message cannot be decrypted by an interceptor. The other viability is authentication. Here the ingress and egress nodes need to confirm the identity of the other party involved in the communication. The final parameter is message integrity (burst integrity). Burst integrity is referred to as validation of the burst. The information transferred from the ingress node should reach the egress node without any modification or change in the burst. Similarly attacker behavior can be defined as “When a node breaches any of the security principles”. However, OBS network is not free of security concern. This is likely to be the case for the majority of traffic served by the OBS layer. In this situation, the entire operation of a network gets disturbed. Several attacks like black hole, wormhole, rushing are to be defined and detect such behaviour of a node. Therefore, it becomes mandatory to define the normal and malicious behaviour of a node. Whenever a node exhibits a malicious behaviour under any attack, it assures the breach of security
principles like availability, integrity, confidentiality etc. An intruder takes the advantage of these vulnerabilities present in the network and attacks the node which breaches the security principles. Due to this vulnerability, the node behaves in malicious manner. The different types of attacks and their impact in optical burst switching network are described in brief:

**Orphan Bursts:** This burst header is responsible for making the WDM channel reservation for its corresponding burst. When the scheduling request is rejected at one of the OBS core routers, there will be no valid optical path set up for the arriving burst. Since the burst is launched, it will be arriving at the input of the core router in any case. At this point, the burst is no longer connected with its header and becomes an orphan burst. As a result, orphan data bursts can be tapped off by some undesirable party, thereby compromising its security (Chen et al. 2009).

**Redirection of Data Bursts:** The one-to-one correspondence between the burst header and its associated burst is implied by the offset time carried in the burst header. Such one-to-one correspondence can be violated by injecting a malicious header corresponding to the same burst. As a result, the route and the destination for the burst can be altered by the malicious header, even though a legitimate path has been set up by the authenticated header.

**Burst control header flooding attack:** When any electronic node is compromised by intruders and later by using that node, the intruder creates multiple copies of the same burst header and advances it to the next node and thereby flooding the next intermediate node with the duplicate copies of the original burst control header.
So the next intermediate node tries to make reservations for these fake burst control headers. Hence overflow of buffers happens at the intermediate core node or, if the wavelength conversion is implemented this bogus burst control header reserves different wavelengths for its respective data burst. Thus the uncompromised nodes will not able to reserve the
resources even when they receive a valid burst header. This attack is called as burst header flooding attack.

**Replay:** Replay attack can be launched by capturing a legitimate but expired burst and transmitting it later, or by injecting an expired burst header to cause the optical burst to circulate in the OBS network, delaying its delivery to the final destination.

**Malicious burst header injection:** The data burst simply follows the optical path and does not possess any idea on routing the information to their intended destination in the OBS network. Hence, as the burst header is set on a schedule and enters the network, it is lost to the unauthorized or illegitimate address. This is mainly due to the lack of absence of authenticating authority in the network. This type of attack is called as malicious burst header injection (Sivasubramanian & Muthuraj 2011).

![Diagram](image)

**Figure 1.6 Malicious burst header injection attack**

**Circulating burst header attack:** This is a type of attack where in two or more compromised nodes are pulled together to form an attack on the OBS network. The burst flow in an already circuited path slows down the
delivery of the data burst to its destination. Under this, the comprised node acts like a master controlling in the predetermined circuit and forwards the burst control header to the intended recipient. This results in the wastage of resources and also in the blockage and unnecessary delay on data burst.

![Circulating burst header attack](image)

**Figure 1.7 Circulating burst header attack**

**Denial of Service:** The OBS core that decides the path of the data burst follows the unoccupied or unused outgoing WDM channels to make their decisions on their path. Whenever there is a non-availability of WDM channel, the burst packets that are to be transited are thrown away. The routers that routed the control packet with their destination do not have a well-defined mechanism to counter check the burst sent has reached their destination or not. This loophole can be used to exploit the network by setting up a malicious burst header that would push WDM channel to be labelled as busy at all times when in reality the network is completely free (Simona Ramanauskaite & Antanascenys 2011).
1.4 MOTIVATION

Optical communication originally found its applications such as transmitting the telephone signals, cable television signals and internet communication. Due to much lower attenuation and interference optical fiber has large advantages over the existing system. The tremendous growth of Internet, demands a large amount of bandwidth for certain applications. This has led to the achievement of a feasible solution for networks that can provide high bandwidth and speed of transmission. The research has led to the birth of transmission of data via optical media that is superior to electronic media. Several methods of transmission have been proposed starting from optical circuit switching to optical burst switching. The latter is still under research and is the most efficient method for network switching.

However, the security issues associated with OBS networks have not been completely analysed yet. Any form of data communication method is credible only when it can provide security. The physical layer of an optical network is vulnerable to a variety of attacks, including jamming, physical infrastructure attacks, eavesdropping, and interception. As the demand for network capacity grows dramatically, the issue of securing the physical layer of optical network cannot be overlooked.

It is envisaged that traffic at the backbone of next-generation optical network will remain in optical domain. In such all-optical network, buffering, switching and routing within the network nodes are performed optically. Network elements such as optical cross-connects and optical add/drop multipliers have full control over all wavelengths. Additionally, they are expected to have a full knowledge of the traffic carrying capacity and the status of each wavelength. With such intelligence, these networks are envisioned as being self-connecting and self-regulating.
The main problem in such all-optical network is the unavailability of optical RAM and technology is not matured for optical processing. As a result of which packet switching is not an appropriate switching technique in all-optical network. Circuit switching is not appropriate because of inefficient bandwidth utilization and is costly in maintaining a circuit. In between the extremes of circuit and packet switching, optical burst switching (OBS) is emerging as the new switching paradigm for next generation optical networks. OBS network can prove to be cost effective interconnection solutions to the ever growing internet. However, OBS network is not free of security issues. Hence the OBS network has to be designed in such a way to ensure the network freedom from the security threats. All this is possible only when a suitable security framework must be designed for every node in the network to face these security threats and vulnerabilities. This work deals with the security issues concerning with OBS networks and proposes a secured edge router model for OBS networks.

1.5 Research Objectives

The proposed research analyses the security threats associated with OBS networks and their solutions. The main objective of this research work is to investigate and understand the pitfalls of security attacks and also providing a suitable security framework design for OBS networks.

The objectives may be summarized as follows:

1. To investigate the security attacks and threats in optical burst switched networks.
2. To select an efficient encryption algorithm for burst confidentiality in OBS networks and enhances its performance using quantum key distribution.
3. To design a suitable quantum key distribution protocol with idealized maximum efficiency and lesser complexity order.

4. To provide burst integrity through enhanced SHA 512 algorithm using quantum keys and analyse its performance with respect to avalanche effect.

5. To provide an efficient and secured burst header authentication algorithm for core node in OBS and analyze its performance with respect to avalanche effect and time complexity.

6. To implement a prototype of unified model of secured ingress router architecture with combined confidentiality and integrity.

1.6 ORGANIZATION OF THESIS

This thesis is organized as follows.

Chapter 1 gives an overview of optical burst switching and the associated security threats and vulnerabilities in the context of which the research work was carried out. Introductory material on optical switching types, possible attacks and security vulnerabilities are presented in this chapter. It also highlights the motivation and objectives of the research work.

Chapter 2 presents a conceptual survey on different types of security attacks and the efforts to prevent these attacks are brought through and presented. This chapter provides a pathway of different attacks experienced by a burst along with the security mechanism and methodology used for strengthening. 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 communicating entities. OBS is regarded as
the most prominent optical switching technology for future internet, because of the unique characteristics of OBS networks, but still facing a degree of security vulnerability associated with the burst.

Chapter 3 deals with the proposed efficient burst encryption algorithm design for Burst confidentiality. It also covers an overview of various existing encryption algorithms and quantum key generation methods. This work employs quantum key based RC4 (stream cipher) to encrypt and decrypt bursts and thereby ensuring the confidentiality of the burst. Although the use of Advance Encryption Standard (AES) algorithm has been proposed for the same issue, by contrasting the two algorithms under the parameters of burst encryption and decryption time, end to end delay it is found that the proposed QKBRC4 provided the better results. This chapter provides a better solution for the confidentiality of the burst in OBS networks.

Chapter 4 describes the security issues associated with optical burst switching with respect to integrity of burst. The proposed Quantum Key based Secure Hash Algorithm (QKBSHA-512) with enhanced round function design provides a good avalanche effect over the conventional integrity algorithms. The conclusion is that the proposed QKBSHA-512 algorithm gives a better avalanche effect than the conventional algorithms. The enhanced round function design uses logic utilization which is equal to the conventional algorithm. The time complexity of the proposed algorithm also presented. More over it is seen that the proposed work is resilient to attacks in optical burst switched networks. This QKBSHA-512 with enhanced round function can be the best choice for real time secure integrity applications of optical burst switched networks.

Chapter 5 outlines the security threats associated with the core router. It also discusses the proposed modified MD5&RC4-4S based header authentication algorithm for burst header. The implementation results indicate
the proposed algorithm is faster than the conventional algorithms and provide better avalanche effect.

Chapter 6 discusses the security issues associated with optical burst switching with respect to the combined parameters confidentiality and Integrity of the data burst. It covers the proposed integrated secured Ingress router architecture design with the use of QKBRC4 and QKBSHA 512 algorithms. The proposed architecture was implemented in diverse FPGA models and the results are presented in this chapter. The results lead to the conclusion that the proposed integrated secured ingress router model is suitable for real time applications in optical burst switched networks.

Chapter 7 summarizes the inferences arrived at from this study, and presents the scope for future research in this field.