A Novel Optical Firewall Architecture for Burst Switched Networks

Maha Sliti, Mohamed Hamdi, Noureddine Boudriga
Communication Networks and Security Research Lab.
University of Carthage, Tunisia

ABSTRACT
Over the last decade, optical networks have experienced growth at a tremendous rate. The rapid increase of bandwidth demand for the transmission of multimedia data has strongly motivated this growth. As a result, optical communications are used for implementing not only backbones but also access networks. Due to the sensitivity of the applications relying on optical networks, security becomes a major concern.

This paper sets the architecture of a firewall node which is able to protect Optical Burst Switched (OBS) networks against physical layer attacks. We first describe the risks threatening OBS networks. Then, we propose an architecture supporting the definition of dynamic rules in order to thwart a specific category of denial of service attacks threatening OBS networks. Finally, we propose a simulation to assess the additional delay resulting from the application of the filtering rules.

1. INTRODUCTION
The amount of research being done in the area of optical communications has dramatically increased over the last years. A large proportion of the telecommunications functionalities including switching, flow control, and buffering are nowadays possible to perform on the optical layer. As a consequence, many applications and services rely on the large bandwidth and high Quality of Service (QoS) provided by optical infrastructures.

Among the most relevant optical infrastructures applications, we can mention the dynamic light-path set-up for sending uncompressed high-definition television (HDTV) signals, grid applications, file transfers, and consumer-oriented grids. Due to the sensitivity of the aforementioned applications, more security requirements for optical networks are necessary. Indeed, some optical networks features can be used by an attacker to analyze traffic, eavesdrop, deny service, etc.

Several approaches have been proposed in the literature to address the protection of optical networks [1], [2]. The major drawback of these methods is that they do not take into consideration the specific features of optical networks. They just translate traditional security mechanisms to optical architectures. Therefore, their efficiency in thwarting threats against All-Optical Networks (AONs) is questionable.

In this paper, we develop a new firewall architecture that operates at the optical layer. We first show that OBS networks exhibit several vulnerabilities especially in the resource reservation protocols. We emphasize on a denial of service attack that prevents legitimate optical nodes from reserving wavelengths at intermediate core nodes of the network. Then, we describe the optical components of the proposed firewall and show how can dynamic rules be implemented. Finally, we assess the impact of the proposed security technique on QoS by estimating the additional delay caused by the use of optical firewall nodes. The key contributions of our work are cited in the following:

• To the best of our knowledge, our work includes the first study of attacks that are specific to OBS networks;
• The proposed firewall node represents the first architecture performing traffic filtering at the optical layer;
• The countermeasure for the denial of service attack conciliates efficiency and minimum impact on QoS.

The rest of the paper is organised as follows. Section 2 provides an overview of the existing researches that have addressed security problems in optical networks. Section 3 introduces new attack techniques for OBS networks. A particular interest will be given to DoS attack that exploits the weaknesses of the existing signalling schemes. The architecture of our firewall scheme will presented in Section 4. Finally, Section 5 concludes the paper.

2. RELATED WORK
This section reviews the basic concepts related to OBS networks including architectural issues, resource reservation and signalling. It also cites the most important applications of OBS communication in order to highlight the sensitivity of serial data exchanged through optical networks. An overview of the research on optical-level security is provided along with an analysis of the shortcuts of the existing approaches.

A. OBS fundamentals
For the sake of clarity, we first discuss the basic aspects of OBS networks. It is widely assumed that all-optical networks represent an ideal solution for next-generation Internet applications [3].

Among various optical switching technologies, optical burst switching (OBS) is considered as one of the most promising optical switching technologies [4], [5], [6], combining the best of both optical circuit and packet switching. In an OBS network, various types of client data (e.g., IP packets) with the same egress node address,
are aggregated at the ingress (an edge node) into bigger entities called data burst, and then transmitted with its control signal on different channels or wavelengths. The control signal consists on a burst header packet (BHP) which is sent ahead of the data burst in order to configure the switches along the burst's route. The BHP carries information about the burst such as, source, destination, offset time, and the burst duration. At the egress node, the burst is disassembled and the individual data packets will be forwarded to the appropriate destinations.

Several signaling protocols have been proposed for optical burst switching networks.

The Tell and Wait (TAW) signaling protocol considers a two-way reservation scheme. A control packet is sent to the path of the burst in order to collect information on the availability of resources. At the destination, an resources assigning algorithm is executed (period of reservation on each node ...). An acknowledgment packet (reply packet) is sent to the intermediate nodes to reserve the necessary resources. If the reservation fails at an intermediate node, a failure packet is sent to the destination. Otherwise if the reply packet reaches the source, the burst will be sent. The Tell-and-Go (TAG) signaling protocol uses a one-way reservation scheme. The data burst is sent immediately after the control packet. TAG considers an immediate reservation technique and an explicit release mechanism. The Just-In-Time (JIT) [8] signaling technique uses immediate reservation, while the Just-Enough-Time (JET) [9] adopts a delayed reservation technique. The delayed reservation technique minimizes. The JIT and the JET signaling protocols uses a one-way reservation scheme and considers an offset time before the start of the data burst transmission.

### B. Security approaches

Several security solutions were proposed to protect optical networks. Among these techniques, we mention the Quantum cryptography [1] that exploits the quantum physics laws to reveal the interception of the information exchanged between two stations. The Quantum cryptography presents two major drawbacks. First, it is based on the principle of the key exchange between two points which makes its extension to mesh networks not feasible. Secondly, it is impossible to apply repeaters or amplifiers to photons which makes the transmission of the keys limited by the distance.

The WISDOM (Wirespeed Security Domains using Optical Monitoring) project [2] aims at developing a reconfigurable photonic firewall. The new system provides a tool to implement security checks and algorithms directly at high-speed optical data communication rates. These photonic firewalls will operate using novel algorithms and protocols, to extract and process wirespeed security information in high capacity multichannel (Tb/s) networks. The algorithms will combine the functionality of optical processing with secondary electronic security approaches to introduce new layers of security analysis. The developed firewall is placed on the Edge network witch separates the access network and the core network in order to filter inbound and outbound wirespeed information. Therefore, the wisdom firewall separates two security domains which is the role of a traditional firewall. Consequently, the developed firewall do not take into considerations the specific features of optical networks and therefore it cannot protect optical networks against optical attacks (attacks on BHP control packets, etc). In this paper, we propose an optical firewall architecture witch is able to protect Optical Burst Switching networks from attacks on BHP packet control resulting in denial of service attack.

### 3. NEED FOR OPTICAL LAYER FILTERING

All-optical networks (AONs) are a viable technology for future telecommunication and data networks, but AONs have intrinsic security differences with respect to existing electronic networks. Some AONs features can be used by an attacker to analyze traffic, eavesdrop, deny service, etc. All-optical technology transport a very high data rates allowing the transmission of an aggregate of more than 10 Tbps and the single channel transmission of 1.28 Tbps over a single fiber. However, the huge bandwidth and transmission rate provided by AONs have often obfuscated their ability to be attacked by malicious entities. In the literature, even though several claim to address the security of optical networks, the study of the vulnerabilities characterizing these networks is nearly absent. In the following, we assess the robustness of OBS networks to various threats. The attacks we will consider break into two categories: hardware attacks and protocol-based attacks.

The first attack category relies on a physical action on the network. For instance, a short attack, which might only affect a small number of bits in a slower electronic network, may affect a very large number of bits in optical communications. Furthermore, the optical transparency in AONs has a negative impact on data transmission. Indeed, this concept allows the signals, that are routed transparently, are amplified but not regenerated at any network component. Furthermore, the QOS may be degraded or even service may be disturbed due to technological limitations of current optical components and devices (Gain competition in EDFA lets malicious high-power optical signals use more upper-state photons so the gain of other user signals will be reduced, etc) [10].

The second class of optical attacks simply exploits security flaws in the signalling protocols. In the frame of this paper, we will focus on the study of a specific DoS attack aiming at overwhelming the resources of an OBS core node. The reasoning behind this threat relies on the flooding principle, which has been extensively covered in conducting classical DoS attacks against the TCP protocol. For example, in the context of the well-known
SYN flooding attack, the objective is to exhaust the resources of the TCP/IP stack at the victim level by making it out of service and therefore unavailable for receipt of legitimate connections. To this end, the attacker tries to generate a massive network traffic. The key weakness exploited by the SYN flooding attack is that, in order to establish a TCP connection with another machine, a three way handshake process is required:

1) A host A sends a SYN packet to a host B,
2) The host B sends a packet SYN-ACK to the host A,
3) The host A responds the host B with an ACK packet.

To achieve the DoS attack, the attacker sends massively SYN packets to the victim and never completes the handshake process (by sending an acknowledgment). As a result, the victim will allocate resources for the malicious connections initiated by the attacker. Therefore, the victim resources will be quickly exhausted and it can not allocate more resources for legitimate connections.

In the optical domain, the DoS attack can similarly occur when a malicious node sends massively control packets (BHP) in the network. Indeed, an optical node will receive a huge number of control packets that requires the allocation of resources (wavelength, etc). The instant of resource allocation depends on the type of the signalling protocol which can be directly after the BHP processing (explicit reservation) or on the receipt of the first bit of the burst (implicit reservation). In both cases, the victim will be overwhelmed and become out of resources. Indeed, the victim will await the arrival of the burst to which it has allocated resources but the expected burst will never arrive. Therefore, the victim node will not be able to allocate more resources to BHP belonging to legitimate connections. Since that the releasing technique can be either implicit (just after transmitting the burst) or explicit (when receiving a release packet), the victim resources will be exhausted and consequently the legitimate control packets will be destroyed due to the lack of resources.

The BHP flooding and the SYN flooding attacks certainly shares some features which consists essentially on the following points:

• As for a SYN packet, a BHP packet allows the connection establishment, in the optical network, by reserving the required resources to transmit the corresponding burst.
• The BHP flooding attack and the SYN flooding attack results in the resource depletion and the unavailability of the victim node.

However, the BHP flooding attack and the SYN flooding attack present some differences that can be summarized in the following points:

• In optical networks, a very high data rates are transported. Consequently, a short attack, which only affects a small number of bits in a slower electronic network, may affect a very large number of bits in optical communications.
• The SYN flooding attack is generally performed against servers while the BHP flooding attack is typically carried out against OBS core nodes. Therefore, the implications of a BHP flooding attack will be more critical than that in the case of a SYN flooding attack since its impact extends the whole communication infrastructure.
• The SYN flood attack is based on the notion of connection state. Indeed, this attack considers the three way handshake mechanism and results on the non receipt of an acknowledgment by the victim node. This is not the case for the BHP flood attack which is not based on the connection state notion.
• The type of resources targeted by the two types of attacks are different. In the case of a SYN flood attack, the exhausted resources will be the CPU, memory and bandwidth. In the case of a BHP flood attack, the resources that will be exhausted will be the output wavelengths and optical memories.

More generally, we can highlight some other differences between optical and traditional attacks including:

• in optical networks attacks can be easily launched from remote sites due to the fact that the propagation loss of optical fiber is very small.
• band-limiting optical filters may be used to discard optical signals outside the operational spectrum and thus mitigate the above mentioned gain competition.

Facing these new attack schemes, the protection techniques that have been covered in the foregoing section are not efficient since they mainly address confidentiality of the data transmitted across optical networks. To thwart these threats, we need a system which is able to enforce access control policies and, mainly, to filter the BHP packets to prevent the occurrence of DoS attacks.

4. PROPOSED OBS FIREWALL ARCHITECTURE

In this section, we present the design of an optical firewall unit that can be added to the novel OBS node architecture in order to accomplish the traditional firewalling functions in optical burst switching networks. The proposed optical firewall unit is composed of the following modules:

A. Security policy management module

The implementation of information security measures is not an end in itself. Thus, the implementation of
a process that allows to establish, review, maintain and improve a security policy is required. This process presents the principal role of the security policy management module. The management of a security policy is a complex process that consists essentially on:

- Risk analysis: it includes essentially a mission statement, asset evaluation and threat assessment,
- Establishment of a security policy in response to a risk analysis phase: consists of selecting the security rules that best fit the requirements of the organization. The security policy rules are based on the routing information maintained by the BHP (source and destination node). The filtering process based on these rules will be achieved by the filtering module which is presented in the next paragraph.
- Model and validate the SP based on the convenient languages: this is done by progressively move from an abstract representation to a more concrete one.
- Store the security policy on optical storage media.
- Update: it guaranties a continuous monitoring of the security policy through scheduled revisions and analyses. This process is essential to practically test the efficiency of the SP. The improve of a SP consists on the insertion or the modification of a filtering rule which requires the analysis of the relationship between this rule and other rules in order to determine the proper order of this rule, reveal rule conflicts and commit the updates.

B. Filtering module

The filtering module apply the security policy rules on the received BHP and data bursts based on the information maintained in the BHP and essentially the routing information (source and destination node). When a BHP packet is received by an optical node and before any treatment of the information contained in the packet (required wavelength, length of the burst, ...), this last consults the filtering module. The filtering module considers the security policy of an optical node to allow a BHP to be processed or not by an optical node according to the source/destination node of the data burst. A BHP can be allowed to continue the resources reservation for its corresponding data burst, as it can be rejected when it demands an unauthorized source or destination node. The filtering module can be stateless or stateful. The stateless filtering module filters packets regardless of connection status to which they belong in opposition to the statefull filtering module that takes into account the connections states. In OBS networks, a stateless filtering module have some application issues. Indeed, when a BHP packet is dropped by a stateless filtering module, the received data burst will be a "directionless" burst as it loss its BHP. Consequently, a statefull filtering module will be more adapted to OBS networks. This module is directly attached to optical virtual memories. Indeed, each time a BHP packet is received, a connection state will be stored in an optical virtual memory for a delay computed based on the offset time and the BHP processing time. A connection state signal maintains information about the source node, destination node, burst length, offset time, data burst arrival time, state. The state of a connection can be one of the following:

- Setup: a BHP packet is received, accepted by the filtering module and have allocated necessary resources to its corresponding data burst.
- Rejected: a BHP packet is received and refused by the filtering module.
- Dropped: a BHP packet is received, accepted by the filtering module and does not succeed to allocate necessary resources to its corresponding data burst. Based on two categories of signaling protocols which are the one-way reservation and the two-way reservation, two cases can occur: the resources reservation failure may be due to the fact of non receipt of a reply packet (acknowledgment) in the case of two-way reservation signaling protocols or the non availability of resources at the data burst arrival instant in the case of one-way reservation signaling schemes.
- Released: a BHP packet is received, accepted by the filtering module and have allocated necessary resources to its corresponding data burst. The corresponding BHP data burst is received and retrasmited so the allocated resources can be either automatically released based on the data burst length contained in the control packet, in the case of implicit release signaling protocol, or after the receive of a control packet from the source indicating the release of the reserved resources, in the case of explicit release signaling protocol.

5. CONCLUSIONS AND PROSPECTS

In this paper, we proposed a new optical node architecture devised to perform optical-layer traffic filtering. Our contribution is two-fold. We have first studied a new category of attacks against optical networks that aim at exhausting the capabilities of the core nodes. Then, we developed an optical firewall based on a matching between the offset time included in the control packet and the actual delay between this packet and the related burst.

Currently, an extension of this work is under development in order to implement more sophisticated security policies using the notion of security state.
REFERENCES