# BHP flooding vulnerability and countermeasure

**Article** *in* Photonic Network Communication · December 2014

DOI: 10.1007/s11107-014-0484-9



**2 authors:**

Maha Sliti
University of Carthage
**16** PUBLICATIONS **31** CITATIONS
SEE PROFILE

N. Boudriga
University of Carthage
**381** PUBLICATIONS **1,328** CITATIONS
SEE PROFILE

Photon Netw Commun
DOI 10.1007/s11107-014-0484-9

# BHP flooding vulnerability and countermeasure

**Maha Sliti · Noureddine Boudriga**

Received: 6 September 2014 / Accepted: 27 November 2014


**Abstract** Optical burst switching (OBS) is a switching technology that can efficiently operate in the optical core network using WDM technology and can also develop the future optical internet. The OBS switching technology presents a trade-off between the two switching technologies: optical circuit switching (OCS) and optical packet switching (OPS). This switching approach increases resource utilization compared with OCS technology and avoids the technological barriers of OPS networks. In OBS networks, many packets are assembled into one data burst at the edge node and a burst header packet (BHP) is sent before the burst transmission by an offset time in order to reserve the required resources in core nodes. This can cause security issues in the network and more specifically denial of service attacks that can occur if a source node is compromised. In this paper, we study a specific denial of service attack which we refer to as "BHP flooding attack", which prevents legitimate traffics from reserving the required resources at intermediate core nodes. We also propose the design of a reconfigurable BHP flooding countermeasure module that allows to counter against this type of attacks in an OBS network.

**Keywords** OBS networks · Denial of service attacks · Optical codewords · Tunable decoder · Virtual optical memory

## 1 Introduction

Over the last years, the amount of researches in the area of optical communications has dramatically increased. This increase has been motivated by the large bandwidth and high quality of service (QoS) demand which are provided by optical infrastructures. These requirements are needed by many applications such as high-definition television (HDTV) signals, cloud computing applications, file transfers, and consumer-oriented grids.

The optical burst switching (OBS) technology presents a trade-off between the two switching technologies: optical circuit switching (OCS) and optical packet switching (OPS). This switching approach increases resource utilization compared with OCS technology and avoids the technological barriers of OPS networks. However, OBS networks present several vulnerabilities, especially in the existing signaling protocols. In OBS networks, many packets are assembled into one data burst at the edge node and a burst header packet (BHP) is sent before the burst transmission by an offset time in order to reserve the required resources in core nodes. This can cause security issues in the network and more specifically denial of service attacks that can occur if a source node is compromised.

In the literature, several approaches [1–11] have studied the protection issue of optical networks. In [12–17], the authors present the security issues and vulnerabilities in OBS networks. More specifically, the denial of service attack, targeting the control packets in OBS networks, was studied in [18,19]. In the present paper, we describe the design of a reconfigurable BHP countermeasure module which is able to detect the denial of service attacks on control packets. The proposed countermeasure optical module is mainly composed of two submodules: (1) the bit pattern matching module and (2) the BHP waiting module. The bit pattern matching module verifies whether the received BHP is sent by a legitimate source node. The bit pattern matching process is optically performed using the concept of optical codewords, which are represented by a sequence of pulses that identify

M. Sliti (✉) · N. Boudriga
Communication Networks and Security Research Lab,
University of Carthage, Tunis, Tunisia
e-mail: slitimaha@gmail.com

Published online: 13 December 2014

unauthorized source nodes. If the BHP does not belong to the source node blacklist, it will be forwarded to the second module which allows to buffer the BHP in a virtual optical memory (VOM) [20], for certain time called timeout. If the timeout is elapsed without the reception of a duplicated copy of the same BHP, the BHP is sent to the next node. In the contrary case, the BHP will be dropped and the address of its source node will be added to the blacklist. With respect to the previously published works, our paper includes the following contributions:

- Our work presents the first study of denial of service attack resulting from vulnerabilities in the resource reservation protocols in OBS networks as discussed in [18].
- The proposed countermeasure module performs the fake control packets filtering optically using the concept of optical codewords. Indeed, an optical codeword is considered to identify each compromised source node in the network which allows the all-optical signal processing of the received control packets at very high bit rates.
- The proposed countermeasure module is reconfigurable since we consider optical codewords and tunable decoders for the bit pattern matching process. Indeed, we use soft-based controlling of optical codewords by considering an optical control unit (CU).
- The proposed countermeasure module is built using components available by current technology. Therefore, the design of the countermeasure module can be implemented.

The rest of the paper is organized as follows. Section 2 presents the OBS network architecture and the optical encoding principle based on optical codewords. Section 3 introduces the principle of the BHP flooding attack that exploits the weaknesses of the existing signaling schemes. Section 4 presents the design of the BHP flooding countermeasure module. The validation of the proposed BHP flooding countermeasure module is presented in Sect. 5 Simulations and experimental results are given in Sect. 6. Finally, Sect. 7 concludes the paper.

## 2 OBS network architecture and codeword management

### 2.1 OBS network architecture

Compared to OCS and OPS optical switching technologies, OBS technology is considered as one of the most promising switching technologies [21–24], since it combines the best from the two technologies. Indeed, OBS networks are more efficient than OCS in terms of wavelength utilization efficiency. It has less stringent requirements for optical devices than OPS, which have to address many issues including optical buffering and low optical switching speed. The bandwidth granularity of OBS networks lies between the bandwidth granularity of OCS and OPS and relaxes relatively technological requirements, which makes it an interesting solution for future optical networks. However, the crucial issue of OBS networks is the high blocking probability which implies a strong need for contention resolution techniques (such as wavelength conversion and fiber delay line buffers).

The structure of an OBS network, described in Fig. 1, consists in a collection of edge and core nodes connected by WDM links. Data bursts composed of multiple packets are all-optically switched at the core nodes. After the construction of a burst in the source edge node and before its transmission of an offset time, a burst header packet (BHP) is sent to configure the switches and reserve the needed resources along the light path. The BHP contains information required to appropriately forward the corresponding burst through the nodes composing the path between the source and destination nodes, such as source and destination address, burst length, and offset time.

Nowadays, the BHP is proceeded at the electronic level due to the lack of fast and scalable optical signal processing technologies. Thus, a core node that receives the BHP converts it to the electrical domain and identifies its destination node. Based on the intended destination of the BHP and a switching table, the appropriate output port is found. If the output port is available at the arrival of the burst, it will be configured to let the data burst pass through. In the contrary case, the core node will consider a contention resolution scheme.

### 2.2 Optical encoding principle

An optical codeword is composed of a sequence of pulses that represent the positions of the information bit "1". When the information bit "0" is transmitted, the transmitter does not produce an optical pulse. An optical codeword is assigned to each node in the OBS network, so that, each node is uniquely identified by its assigned codeword. This mapping is similar to an address in the traditional network. In our case, a codeword can be considered as a vector of integers, where each element identifies the position of a pulse (bit "1") in the codeword. Thus, the considered generation process of codewords is based on the lattice point theory and is performed as follows: Consider a $m \times k$ integer lattice $L = Z_m \times Z_k$, which elements are labeled by points from the set $V = 1, 2, ..., mk$. Using a simple linear mapping function defined as:

$$l : L \rightarrow V, l(x, y) = mx + y + 1 \quad (1)$$

where $0 =< x <= k - 1$ and $0 =< y <= m - 1$.

The codewords are also represented as lines connecting points of the rectangular integer lattice. The subset of points is referred to as lines, and the code spaces are defined as the

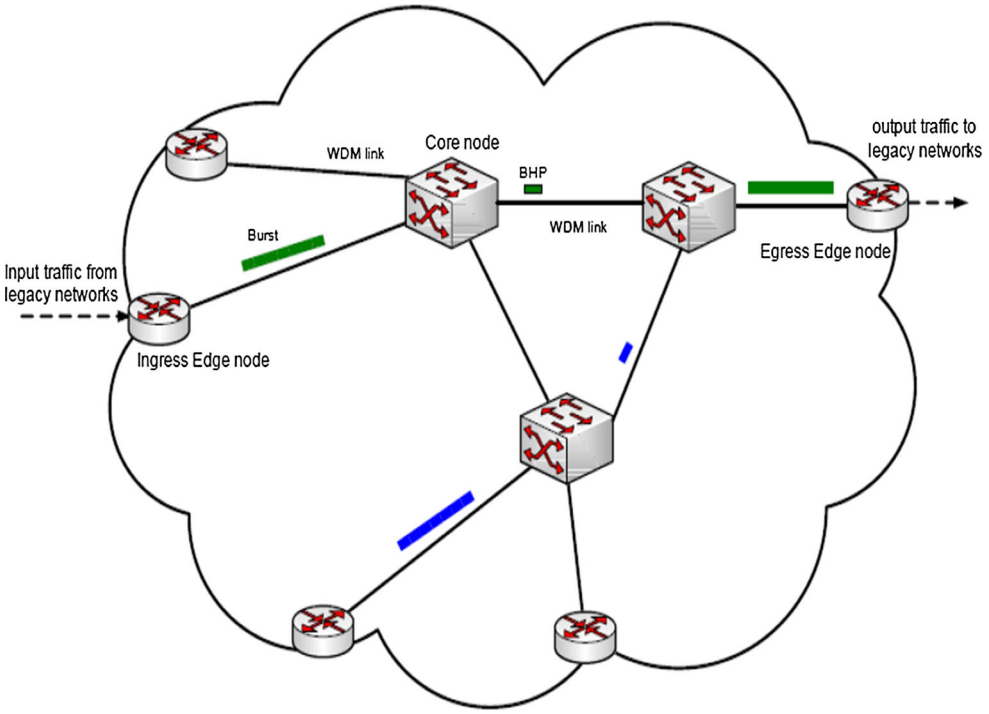


**Fig. 1** OBS network architecture

sets of lines of different slopes. A line with a slope $s$, where $0 \leq s \leq m-1$, starting at the point $(i, j)$, contains the following set of points:

$$(i; j + (s.imod(m)) : 0 \leq i \leq k-1; 0 \leq j \leq m-1 \quad (2)$$

Thus, for every slope $s$, the $m$ codewords that can be obtained are $v = v_1, ..., v_m$, where $v_j = mi + j + (s.imod(m)) + 1; 0 \leq i \leq k-1$ for every $0 \leq j \leq m-1$. It can be shown, as in [25], that this method generates codewords with length equal to $mk$ and weight $k$. The weight represents the number of bits "1" in a codeword. This is a very important parameter because it has been shown that it identifies the maximum value of the autocorrelation between codewords and, hence, reflects the capability of the routing approach to separate traffics intended for specific destinations. It is noteworthy that for every slope, the codewords obtained through the aforementioned process are orthogonal. According to this reasoning, every codeword $v_j$ can be represented as an integer vector $v_j = v_j^0, v_j^1..., v_j^{k-1}$ where $j \in 1, 2, ..., mk$ and $v_j^i$ is the $i^{th}$ bit in the optical codeword $v_j$.

### 2.3 Codeword-based burst switching

In this paper, we present the design of a countermeasure module that detects the occurrence of denial of service attacks on control packets. This module is mainly based on optical codewords that allows the OBS based on their source addresses. Indeed, the received BHP must be sent by a legitimate source node. In the contrary case, the received BHP must be dropped. In order to perform the optical switching process, a codeword is associated with an unauthorized source address in order to optically filter erroneous control packets.

Therefore, a core node, which implements a countermeasure module, performs mainly two optical operations, which are the optical codeword matching and the deviation of control packets to the adequate direction. The received codeword is split to a set of decoders; if a codeword is matched by a decoder, an optical switching gate will be activated by a pulse to forward the control packet to the next core node. Indeed, each decoder is configured with a codeword associated with unauthorized source address.

As shown in Fig. 2a, an optical encoder is composed of a $1 \times w$ optical power splitter, $w$ fiber-optic delay lines and a $w \times 1$ optical power combiner. The delay of the $j^{th}$ delay line is $i_j\tau, 0 \leq i_j \leq N-1$, where $N$ is the codeword length, $w$ is the code weight, and $\tau$ is the width of an optical pulse in the codeword. The light source sends an optical pulse with time-width $\tau$ into the optical modulator. The optical modulator outputs an optical pulse when the data bit is "1," and the optical modulator outputs nothing when the data bit is "0." Then, the optical pulse corresponding to the data bit "1" is encoded by an optical encoder whose output is an optical orthogonal codeword. In the case of a data bit "0," nothing is output from the optical encoder.

As depicted in Fig. 2b, an optical decoder has the same structure as its corresponding encoder except that the delay of its $j^{th}$ delay line is changed into $(N-1-i_j)\tau, 0 \leq i_j \leq N-1$.

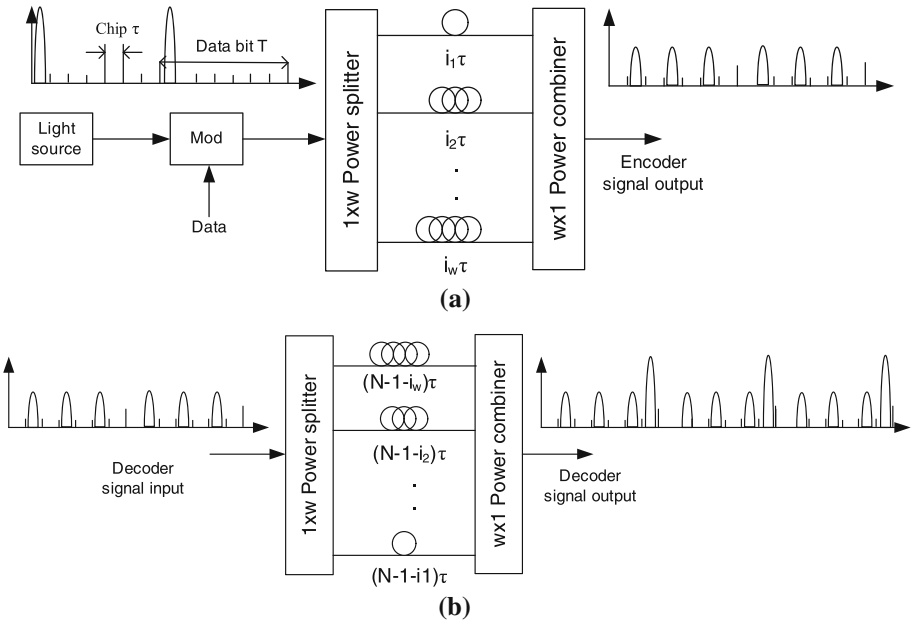


**Fig. 2** All-optical encoding/decoding, **a** all-optical encoder, **b** all-optical decoder

## 3 BHP flooding attack

In OBS networks, the control header is transmitted before the data burst to reserve the required resources along the light path. After an offset time of the control packet transmission, the data burst is transmitted to be all-optically switched through the network. The separation between control and data allows the optical processing of the data burst.

In the frame of this work, we are interested to a specific denial of service attack that aims at overwhelming the OBS core node resources. This threat relies on the flooding principle, which has been extensively studied in classical DoS attacks against the TCP protocol. For example, the well-known SYN flooding attack aims at overwhelming the resources of the TCP/IP stack at the victim level by making it out of service and, therefore, unavailable to accept legitimate connections. This attack is achieved by the generation of a massive number of SYN requests without completing connection setup.

Similarly, the burst headers can be exploited by a denial of service attack when a malicious node sends off a succession control packets in the network. This attack, which we refer to as "burst header packet (BHP) flooding attack", belongs to the protocol-based attacks category and exploits security flaws in the signaling protocols. In particular, if a source node is compromised by an intruder, it creates multiple copies of the same burst header packet and forwards these copies to the next core node, as illustrated in Fig. 3. Therefore, an intermediate node which receives a succession of control packets, will be flooded and tries to make reservations for these fake burst header packets. The resource allocation can be directly sent after the BHP processing or on the receipt of the first bit of the data burst as illustrated in Fig. 4, depending on the type of the considered signaling scheme. In both cases, the target will be flooded due to the allocation of resources to an expected burst that will never arrive. On the receipt of legitimate control packets, the victim node will not be able to allocate the required resources. The resource release can be either implicit (just after transmitting the burst) or explicit (when receiving a release packet), and consequently, the victim exhausted by erroneous control packets will drop legitimate control packets.

The BHP flooding and the SYN flooding attacks share mainly the following features:

- A control packet establishes a connection in optical networks such as a SYN packet in traditional networks. This is achieved by the reservation of the required resources to transmit the corresponding data burst.
- The BHP flooding attack, such as the SYN flooding attack, results in the exhaustion of resources and the unavailability of the victim node.

However, the two denial of service attacks present some differences that can be summarized as follows:

- In optical networks, high data bit rates are transmitted; therefore, a short attack may affect a very large number of bits in optical communications contrary to a slower electronic network.
- The SYN flooding attack generally considers servers as targets, while the BHP flooding attack is typically per-

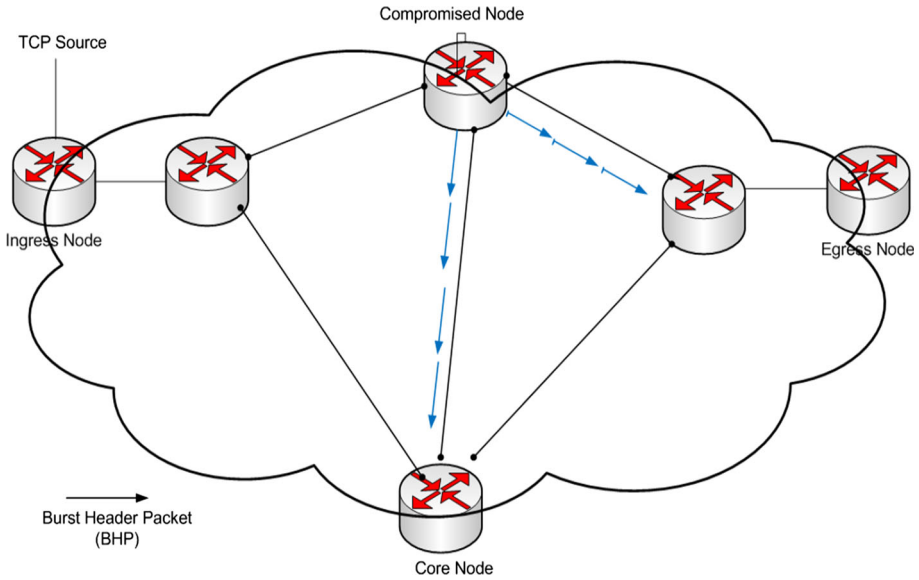


**Fig. 3** BHP flooding attack

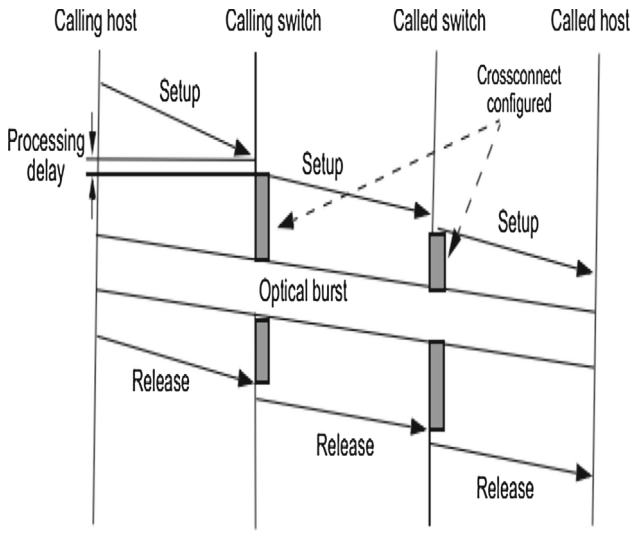


**Fig. 4** Explicit setup and explicit release

formed against optical core nodes. Consequently, the occurrence of a BHP flooding attack is more critical since its impact extends the whole communication infrastructure.

- The SYN flooding attack, contrary to the BHP flooding attack, considers the connection state concept based on the three-way handshake mechanism which results on the non-receipt of an acknowledgment by the victim node.
- The type of resources targeted by the two types of attacks are different. the exhausted resources in the case of a SYN flood attack can be the CPU, memory, and bandwidth. However, in the case of a BHP flooding attack, the exhausted resources can be the output wavelengths and optical buffers.

## 4 Attack detection and countermeasure

Based on the BHP flooding attack that have been described in the foregoing section, two key differences can be noticed between the study of traditional attacks and all-optical attacks.

- DoS attacks' countermeasures proposed for traditional networks cannot be applied to OBS networks. Indeed, in all-optical networks, we need to perform countermeasures in the optical layer due to the high data bit rates transmitted by this type of networks contrary to traditional networks in which countermeasures are electronically implemented.
- The DoS countermeasure module can exploit some intrinsic components of existing OBS core nodes, such as delaying and wavelength conversion modules.

To counter against the BHP flooding attacks, we need to filter the erroneous control packet transmitted in the network. In this section, we present the design of the BHP flooding countermeasure module, illustrated in Fig. 5, which can be considered as an extension of an OBS core node architecture in order to counter the occurrence of BHP-based DoS attacks in OBS networks. The proposed module can be included into a set of core nodes depending on the size of the OBS network.

The BHP flooding countermeasure module is mainly composed of:

- Bit pattern matching module: This module allows/denies a control packet to be processed and performs necessary resource reservation for its corresponding burst. Based on

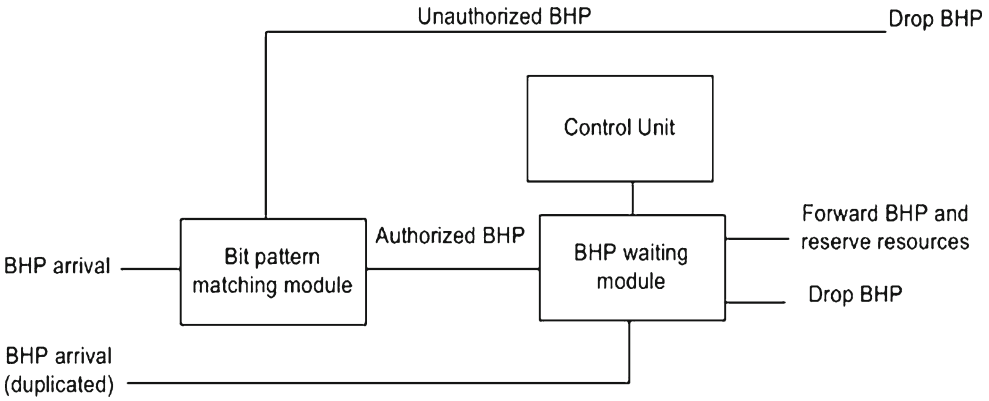


**Fig. 5** BHP flooding countermeasure module

the routing information maintained in the BHP and in particular the source address, the bit pattern matching module analyzes the control packet in order to filter unauthorized nodes. An unauthorized control packet will be automatically dropped, and the list of the unauthorized addresses will be updated. In the contrary case, the control packet will be buffered in the BHP waiting module.

- BHP waiting module: This module buffers a control packet for a maximal delay, called timeout. If during the timeout a duplicated BHP copy is received, its respective burst does not arrive before the elapsed timeout, the control packet will be dropped and considered as a fake control packet. And the list of the unauthorized addresses will be updated. In the contrary case, the control packet will be forwarded to the next core node and considered as a legitimate connection.

### 4.1 Bit pattern matching module

The design of the Bit pattern matching module is illustrated in Fig. 6. At the reception of the BHP, the codeword associated with the core node source address is extracted and split to a set of tunable decoders. Each decoder is configured by the CU with a codeword associated with an unauthorized source address. An optical codeword is composed of a sequence of pulses that represent the positions of the information bit "1". When the information bit "0" is transmitted, the transmitter does not generate an optical pulse. If the threshold detector detects a pulse, then an SOA gate will be activated in order to drop the fake control packet. In the contrary case, the threshold detector activates another SOA gate in order to forward the BHP to the waiting module.

A codeword decoder, which is the main component of the bit pattern matching module, allows the matching of a codeword optically without the O/E/O conversion. The design of a tunable decoder was proposed in [26] in order to implement an optical filtering technique based on codewords. In each loop, an optical pulse is injected to be confined in the fiber until it performs the required number of rounds to place it in the positions of a '1' bit in the optical codeword. Therefore, the number of ones in the codeword defines the number of needed optical loops. Thus, codewords can be easily modified by controlling the number of rounds performed by the optical pulse in each optical loop contrary to classical techniques [fixed length optical delay lines (ODLs) and fiber bragg gratings] which need a physical intervention. As we can notice, the considered approach allows soft-based controlling of optical codewords by considering an optical CU. A codeword is considered as a vector of integers of $k$ elements that presents the positions of 1s in the codeword. Thus, an optical codeword is composed of optical pulses transmitted in positions of 1s in the code sequence. This can be achieved by considering an on–off keying technique and modulating the label by a Gaussian optical pulse signal and a Mach-Zehender modulator. The tunable decoder, illustrated in Fig. 7, generates an optical pulse when receiving a codeword that matches a configured codeword. The decoding operation is performed by delaying optical pulses that compose the received codeword until they superpose in the last chip interval. A chip is the delay of an optical pulse.

### 4.2 BHP waiting module

The BHP waiting module verifies whether a control packet is associated with an effective data burst or not. This is performed based on the delay of the BHP optical signal in an ODL in order to detect the arrival of duplicated copies of the same BHP. If a duplicated copy of the BHP does not arrive during a waiting delay that we call timeout, the BHP will be considered as a legitimate BHP. In the contrary case, the BHP will be dropped, considered as a fake BHP, and its source address will be added to the unauthorized source node list.

In a proposed design, the choice of the timeout is critical since it results on the drop of the control packet and the update of the list of the fake optical nodes. Due to the

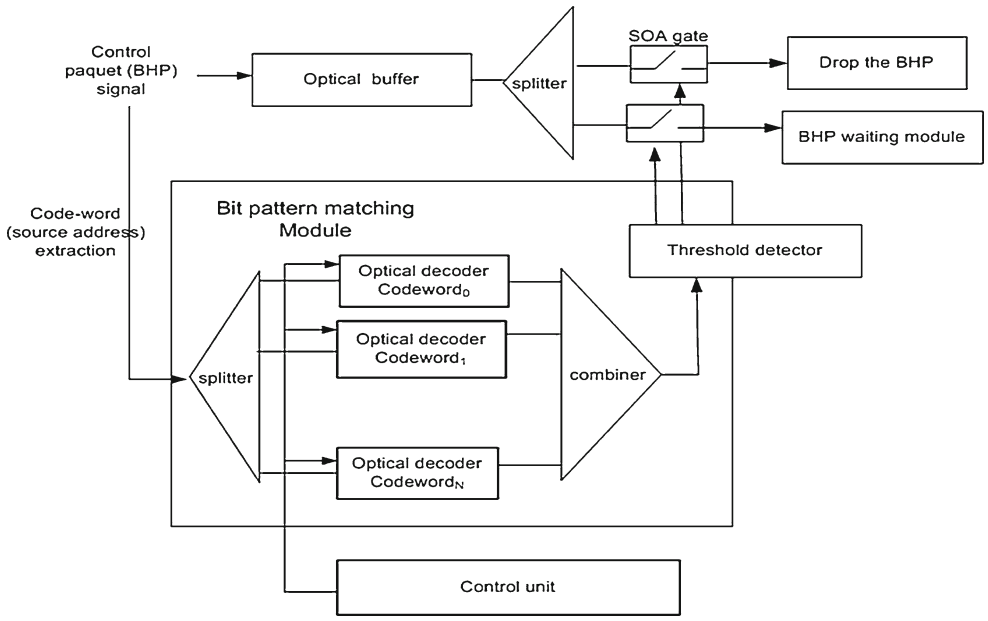


**Fig. 6** Bit pattern matching module

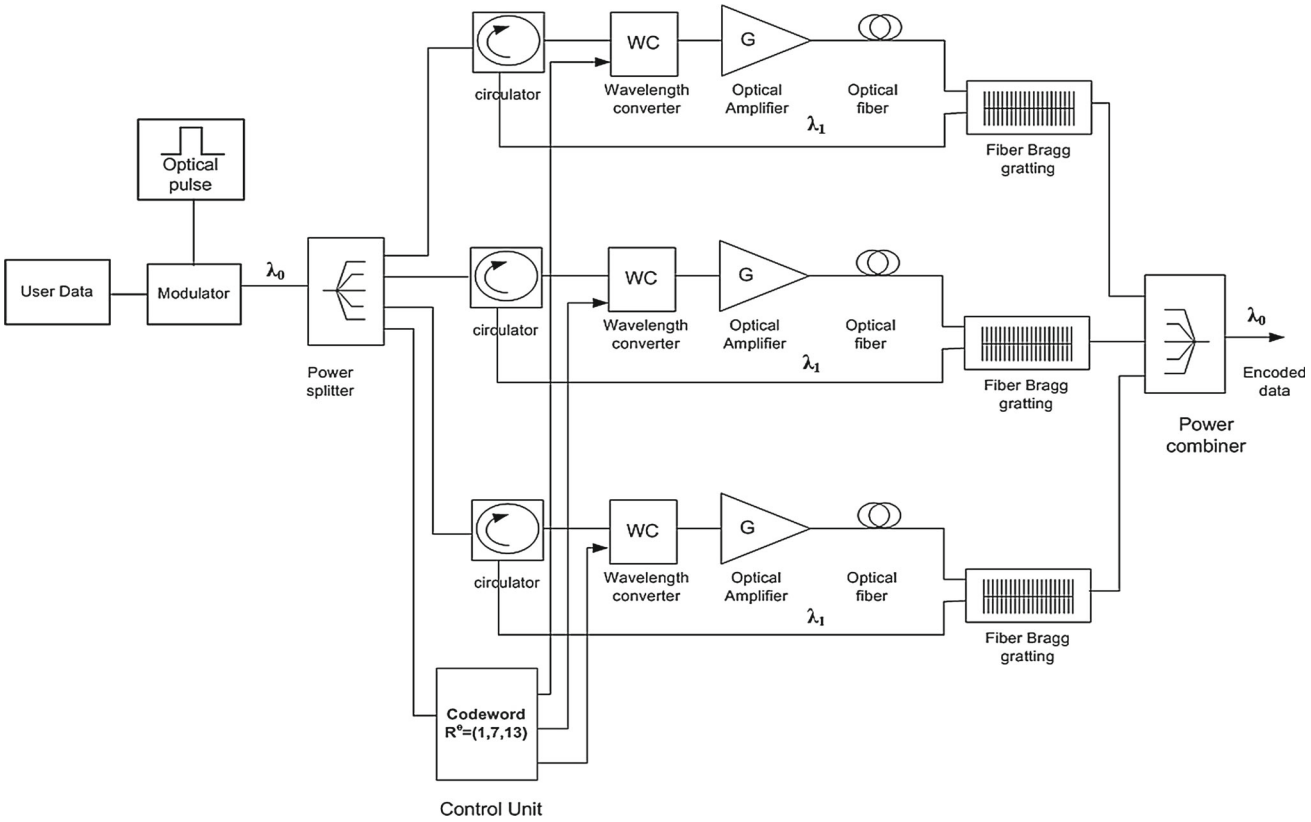


**Fig. 7** Tunable optical decoder architecture

additional delays introduced by the BHP waiting module in order to detect fake control packets, the BHP flooding countermeasure module will be only implemented in some core nodes and not all nodes in the network.

The BHP waiting module design, which is described in Fig. 8, is based on the VOM proposed in [20]. The VOM is organized on two optical delay loops (ODL). The first loop is used to delay the data units, and the second amplifies it,

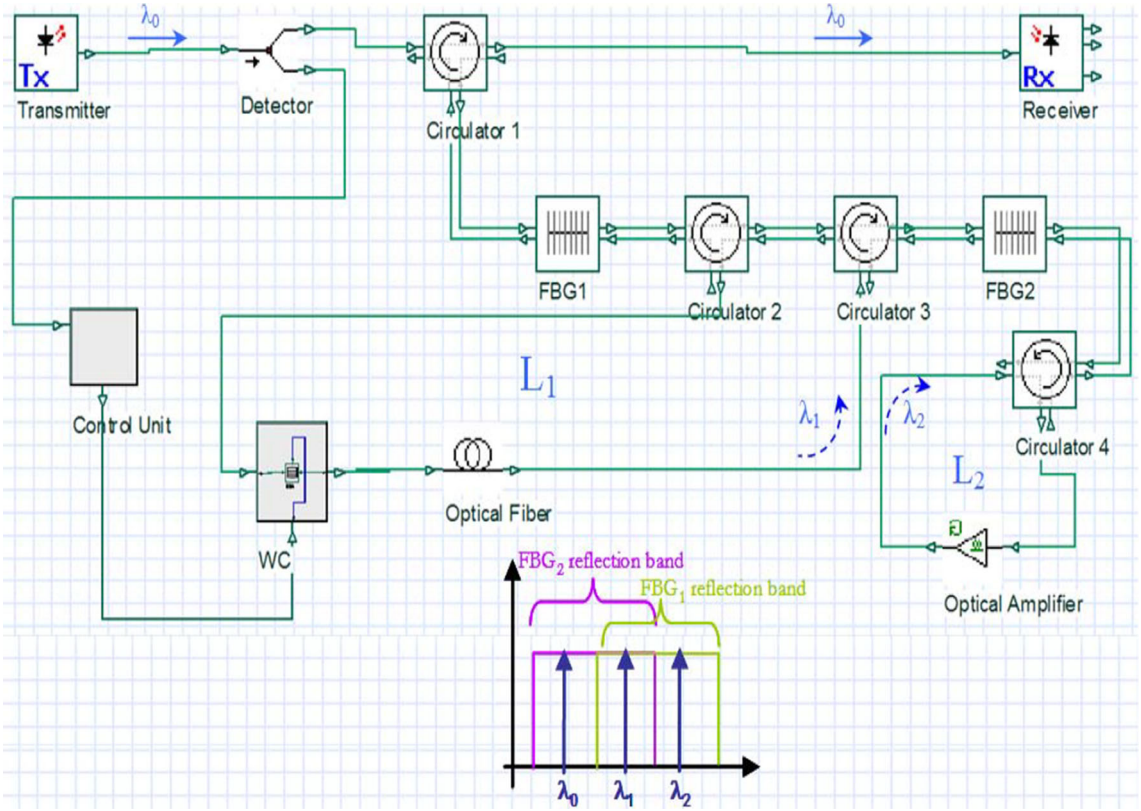


**Fig. 8** BHP waiting module architecture

when needed. At the entering of the first loop (L1), a fiber bragg grating (FBG1) is considered in order to force the optical signal in loop L1 to keep circulating if its wavelength occurring in the reflection band. An input signal arrives first at a passive optical coupler that informs the CU of the signal arrival. Then, the input signal is led to the second arm of the first circulator, where it is amplified. It passes across the first FBG, as its wavelength is external to the reflective Bragg band (say $\lambda_{signal} = \lambda_0$). Arriving at the first arm of the second circulator, the signal gets out from the second arm. The wavelength converter, here a SOA-based system, modulates its continuous wave input and outputs a signal on a different wavelength. When it detects the signal for the first time, it shifts the signal wavelength to a wavelength in the reflection band of FBG1 and FBG2 ($\lambda_{signal} = \lambda_1$) to confine the signal within the first loop L1. The CU evaluates whether an amplification operation is needed according to the information previously collected. When required, the CU shifts the signal wavelength out of the reflection band of the second FBG ($\lambda_{signal} = \lambda_2$) to relay the packet to the second loop (L2) where it is amplified. When the delay duration is elapsed (or more generally, when the QoS of service is decreased), the CU commands the wavelength converter to shift the signal wavelength to $\lambda_0$. As a result, the wavelength signal leaves the first FBG reflection band ($\lambda_{signal} = \lambda_0$) and the signal passes to the third arm of the first circulator.

Compared to a single ODL loop implementation, the proposed two-loop structure increases the maximum time period an optical signal could be delayed. This is because it minimizes the number of amplifications which avoids signal quality degradation. Indeed, the confinement of the signal in the first loop (L1) causes some distortions due to the signal propagation through various components of the virtual memory. Consequently, the number of turns of the signal in loop L1, which depends on the parameters causing the distortion and the fiber length, cannot exceed a maximum value because of unacceptable signal loss. Furthermore, the number of amplifications of the signal cannot exceed a maximum number to preserve it from unacceptable degradation of the signal-to-noise ratio (SNR).

A main component of the BHP waiting module design is the CU that decides about the path to be followed by the delayed signal. In [20], an all-optical design of the CU is proposed. Thus, the CU will deliver three optical signals at the moments to pilot wavelength conversions. A first signal using the wavelength $\lambda_1$ is generated the command the conversion from the original wavelength $\lambda_0$ of the optical corresponding to the data segment to $\lambda_1$ which allows its confinement in the first loop (L1) and starting the delay. When the data signal

power reaches a weak level, it should leave the loop (L1) and injected in the second loop (L2). This is performed by commanding the wavelength converter by an optical signal that uses the wavelength $\lambda_2$ which leads to inject the data signal in the second ODL loop (L2) where it is amplified. After performing the predefined delay, the CU generates a third signal using the wavelength $\lambda_0$ at the exit moment to allow the data optical signal to get out from the first ODL loop (L1). Thus, the CU architecture encompasses three main components. The first is a calculator that compute the number of rotation in the first loop and the number of amplifications needed in the second loop. The second component is the synchronizer that detects the arrival of an optical signal corresponding to a data unit (optical segment in our context). The last component is a multi-wavelength laser source to generate optical signals that use wavelengths $\{\lambda_0, \lambda_1, \lambda_2\}$ to command the wavelength converter. The implementations of this laser source could be based on optical flip-flop or laser neural network (LNN) technologies [27].

OBS networks are subject to several novel attacks that need to be classified. Among these attacks, several DoS attacks can be studied and investigated (DoS attack based on the modification of codewords, Burst replay, etc). In this section, we have studied a new denial of service attack that prevents legitimate connections to reserve the needed resources at intermediate core nodes. This attack, which we refer to as "BHP flooding attack", occurs when a malicious node sends a succession of control packets to the core nodes. This raises the need to develop a minimal number of optical circuits that should be reconfigurable to detect a maximal number of DoS attacks. Indeed, the proposed countermeasure module can be adapted in order to counter other types of DoS attacks such as the burst replay attack that occurs when a compromised node sends multiple copies of the same burst.

## 5 System validation

In this section, we discuss the performance of the proposed BHP flooding countermeasure module based on these properties: correctness, scalability, and addition of unauthorized addresses.

### 5.1 Correctness

Correctness consists in filtering correctly BHPs so that erroneous BHPs should be rejected. In the proposed countermeasure module, we consider an optical buffer called the VOM, proposed in [20]. The VOM is used to delay the traffic payload during the bit pattern matching and the BHP waiting processes. Depending on the decision of the proposed countermeasure module, the BHP will be forwarded to the next core node and the resources are reserved to the burst or dropped. The VOM has an effect on the correctness of the countermeasure module decision. Indeed, the drop of a BHP can be the result of the countermeasure module decision or a degradation of the BHP signal quality when circulating in the VOM. Indeed, if the number of turns in the VOM exceeds the maximal number of turns allowed in the VOM without the loss of the optical signal quality, the optical signal will be discarded, which affects the correctness of the countermeasure module decision. In this case, the BHP signal will be filtered due to the considerable degradation of its quality and not due to the filtering decision.

### 5.2 Scalability

The scalability of the proposed countermeasure approach can be evaluated in terms of signal quality (attenuation), the matched number of unauthorized addresses, and the number of intermediate core nodes. The BHP signal degradation in the VOM depends on the maximal number of unauthorized addresses to be verified by the bit pattern matching module. Indeed, the number of turns in the VOM depends on the matching delay, which is related to the number of unauthorized addresses to be verified. We can evaluate the signal degradation resulting of the turn number in the VOM by evaluating the SNR and Q parameters of the output signal. The Eq. 3 listed below gives the SNR expression after $i$ turns in the loop, where $A_k$ is the total loss after $k$ turns in the first loop L1, $P_{in}$ is the input signal power, $\eta_{SP}$ is the ratio of electrons in higher and lower states, $h$ is the Plank's constant, $\Delta f$ is the bandwidth that measures the noise figure, and $G_{EDFA}$ is the EDFA gain. The Eq. 4 gives the logarithmic $Q$ factor expression after $i$ turns in the loop, which is deduced from the $SNR_i$, and where $B_0$ is the optical bandwidth of the photodetector and $B_c$ is the electrical bandwidth of the receiver filter.

$$SNR_i = \sqrt{\frac{B_0}{B_c}} \frac{\frac{P_{in}.(A_k.G)^i}{2.\eta_{SP}.h.B_0.\Delta f.(G^i_{EDFA}+G_{EDFA}-2)}}{2.\left(1+\sqrt{\frac{P_{in}.(A_k.G)^i}{2.\eta_{SP}.h.B_0.\Delta f.(G^i_{EDFA}+G_{EDFA}-2)}+1}\right)} \tag{3}$$

$$Q_i(dB) = 20log\left(\sqrt{SNR_i\frac{B_0}{B_c}}\right) \tag{4}$$

The total loss $A_{tot}$ of the BHP signal after performing the BHP flooding countermeasure process is given by equation:

$$\begin{aligned} A_{tot} &= A_{matching} + A_{waiting} \\ &= (i_{matching} + i_{waiting}).(2A_{fbg} + A_{fib}L + 4A_{cir}) \\ &\quad + 4A_{wc}, \end{aligned}$$

where $A_{matching}$ is the optical signal attenuation in the bit pattern matching module, $A_{waiting}$ is the optical signal attenuation in the BHP waiting module, $i_{matching}$ is the number

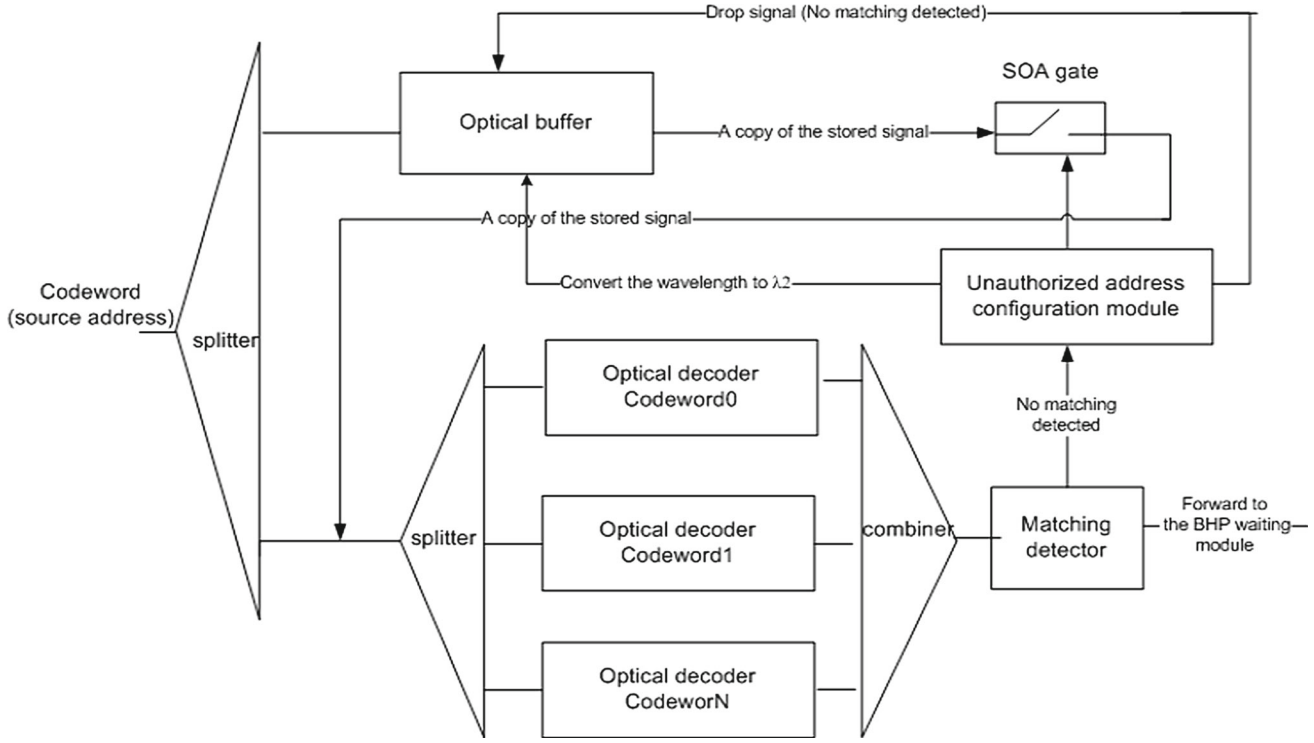


**Fig. 9** Bit pattern matching module reuse

of turns in the VOM in the bit pattern matching module, $i_{waiting}$ is the number of turns in the VOM in the BHP waiting module, $A_{fbg}$, $A_{wc}$, $A_{fib}$ and $A_{cir}$ are, respectively, the attenuation caused by the fiber bragg gratings, wavelength converter, fiber, and circulator.

We can notice that the signal attenuation depends on the number of unauthorized addresses to be verified in the bit pattern matching module and the waiting timeout in the BHP waiting module. Furthermore, the number of intermediate core nodes that includes a BHP countermeasure module is critical. Indeed, the BHP signal quality decreases when this number increases. Thus, we must compromise between security and signal quality aspects.

### 5.3 Addition of unauthorized addresses

In the case where the number of unauthorized addresses to be verified by the bit pattern matching module is equal to the number of optical circuits used for the matching process, an optical circuit will be configured to verify the newly added unauthorized address. In the contrary case, it is not feasible to add a new optical circuit for each added unauthorized address. To resolve this issue, we improve the proposed countermeasure module design as described in Fig. 9. This module allows the reuse of optical circuits in the case where the number of unauthorized addresses $n$ to be verified exceeds the number of available optical circuits $s$ used for the matching process. Indeed, the maximal number of iterations to be performed is equal to $\lceil \frac{n}{s} \rceil + 1$.

At the reception of the BHP, the codeword corresponding to an unauthorized source address will be extracted and split to a set of initially configured optical circuits. In the first case, after the matching verification of the first set of unauthorized addresses, the matching detector detects a pulse in the output of the combiner, which means that at least one unauthorized address is matched. In this case, the matching detector allows the delayed BHP to be sent to the BHP waiting module. In the second case, the matching detector does not detect a pulse in the output of the combiner which means that no address is matched. In this case, the matching detector commands the address configuration module to configure the set of optical circuits with the following set of unauthorized addresses and commands the SOA gate in order to have a copy of the delayed optical codeword. This latter will be split to the new configured optical circuits. This loop is repeated until the complete list of unauthorized addresses is verified. In the case where no matching is detected, the delayed BHP will be sent to the BHP waiting module. In the contrary case, the delayed BHP will be dropped.

SOA gates are considered as high-speed optical switches that can either be optically or electrically controlled. One of the most desirable properties of the considered SOA gate is the fast switching speed. Depending of the type of the SOA gate and the key temporal parameters of the SOA transit time, we obtain different switching window widths as illustrated in

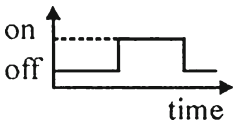


**Fig. 10** Switching window

Fig. 10 [28–30]. For high-speed processing, short switching window is used. In order to have a copy of the codeword corresponding to the unauthorized source address in each loop, we have considered the design of the VOM [20] and added a new wavelength $\lambda_3$. The proposed optical buffer, illustrated in Fig. 11, is organized in three ODL loops.

## 6 Simulations and experimental results

This section is devoted to the performance evaluation of the proposed BHP flooding countermeasure module. We have divided our study into two parts. The first set of experiments is devoted to studying the capacity and limits of the proposed countermeasure module. The second set is used to test the security level provided by the proposed BHP flooding countermeasure module.

### 6.1 Signal quality control and limit

In this subsection, we assess the performance of the proposed countermeasure module by evaluating the effect of the BHP waiting delay on the output signal quality. To this objective, we consider Optiwave Optisystem as a simulation platform. The optical transceiver is modeled as a User Defined Bit Sequence Generator with a 10 Gbits/s transmission bit rate which generates an optical codeword. The input optical codeword is split into $n$ decoders in order to verify whether its corresponding traffic stream is allowed to be sent to the next core node or not. During the filtering process, the data signal will be delayed in an ODL. The filtering delay depends on the length of the optical codeword and the number of optical codewords to verify within the decoders. Each decoder is configured with an unauthorized source node address. If the input optical code matches an unauthorized source node address, then its corresponding BHP will be dropped. In the contrary case, the BHP will be sent to the BHP waiting module.

In each simulation, we vary the buffering delay of the data signal in order to evaluate the impact of the filtering process on the output signal. The number of rounds in the loop that the signal can experience cannot exceed a certain value because of unacceptable signal loss. The number of amplifications cannot, however, exceed a certain number due to unacceptable degradation of the SNR. The quality factor Q, the eye diagram, and the bit error rate are used as performance estimators for the simulated waiting module.

Figure 12 illustrates the output eye diagrams obtained after 5, 8, 10, and 12 rounds in the loop, when observing the received signal at the output of the receiver. The eye diagram highlights the distortion of the signal transmitted due to the time delay in the waiting module. Distortions shown on the eye diagram demonstrate that we can memorize arrived BHP packets for a maximal delay equal to T12 without reaching an unacceptable distortion value.

Figure 13 illustrates the Q factor curves for four delays: 5, 8, 10, and 12 rounds in the loop. The maximum Q factor decreases, while the number of rounds increases. Indeed, The maximum Q factor decreases from 40 dB for 5 rounds to 18 dB for 12 rounds. Thus, we must have a compromise between the number of rounds that an optical signal can perform in the BHP waiting module and the quality of the output signal.

Bit error rate (BER) measurement is the fundamental measurement of the quality of the fiber-optic communication system we use. It measures the system's probability that

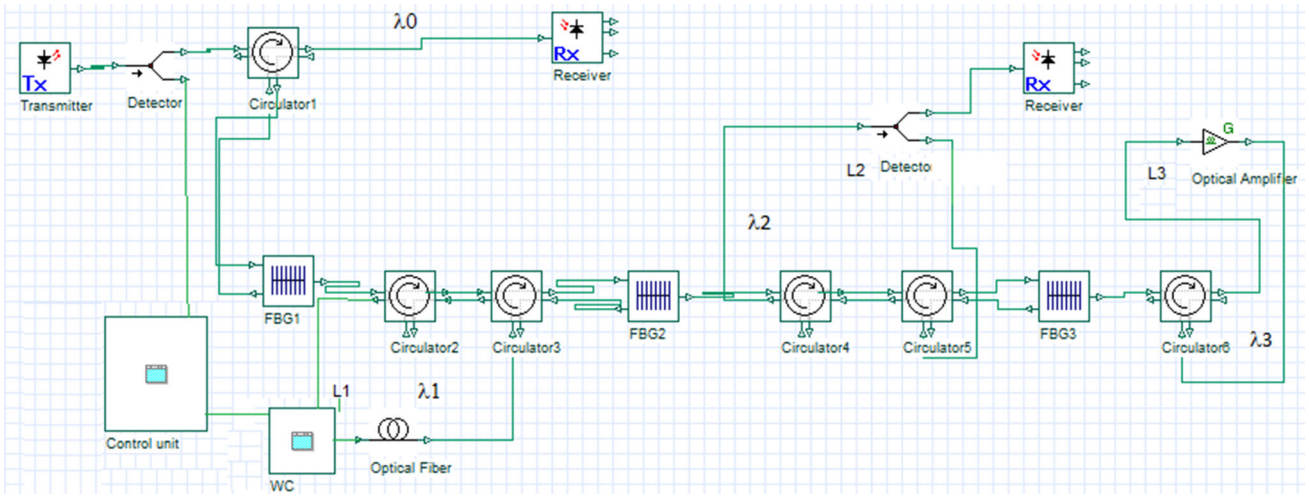


**Fig. 11** Optical buffer design

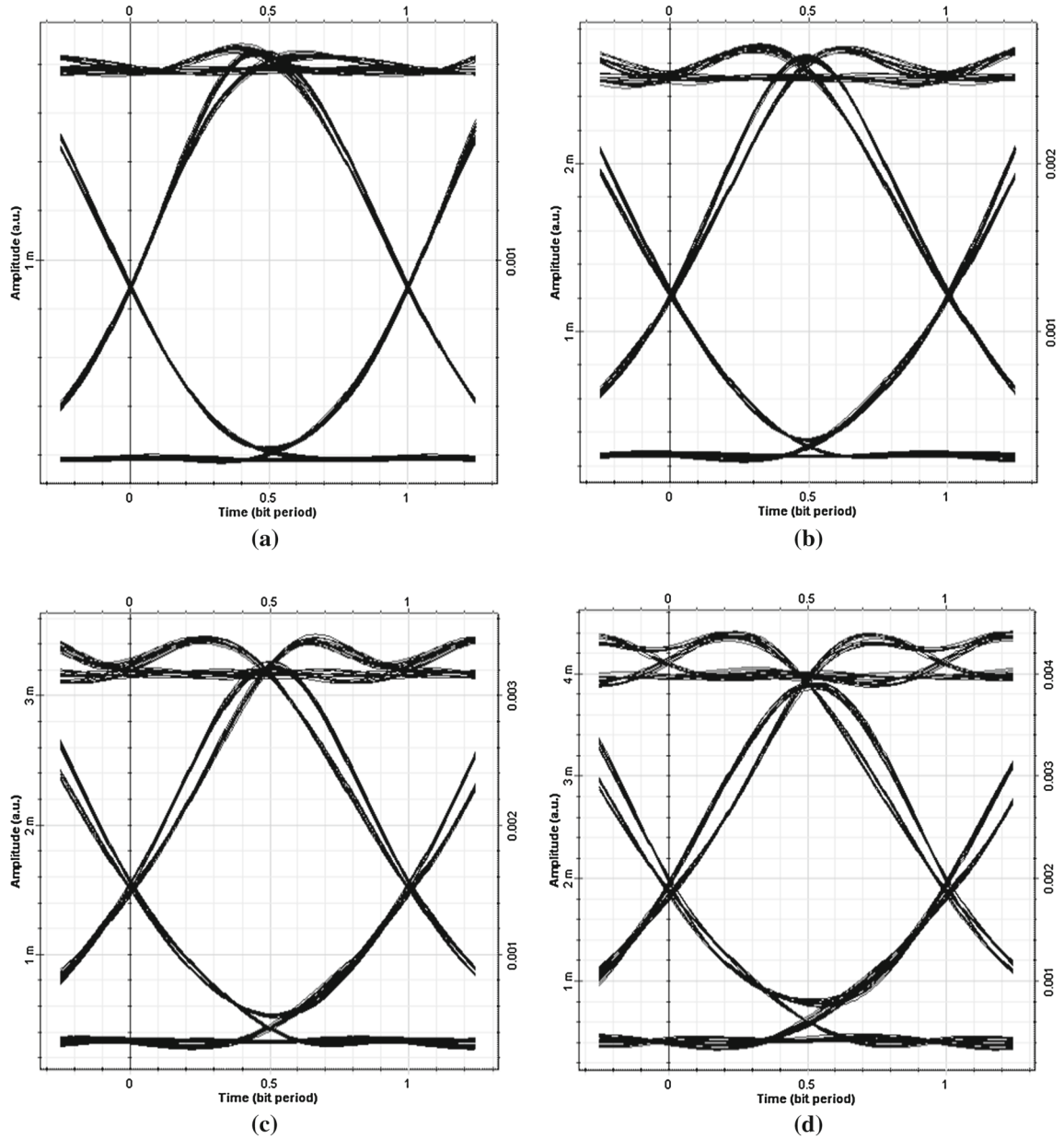


**Fig. 12** Eye diagrams for different filtering overheads, **a** filtering delay: 5 tours, **b** filtering delay: 8 tours, **c** Filtering delay: 10 tours, **d** filtering delay: 12 tours

transmitted bits will be correctly received as logic ones and zeros. The typical acceptable BER levels range from $10^{-9}$ to $10^{-12}$. A BER of $10^{-9}$ means that 1 bit out of every $10^{9}$ bit is, on average, read incorrectly. By considering the Optisystem BER analyzer, we measure the minimum bit error rate (MBER) for four delays: 5, 8, 10, and 12 rounds in the loop. The results are as follows:

- 5T : MBER of $10^{-165}$
- 8T : MBER of $10^{-136}$
- 10T : MBER of $10^{-63}$
- 12T : MBER of $10^{-25}$

We therefore notice that the proposed optical flow filtering mechanism does not affect the quality of the signal for a reasonable number of loops (12T) in the BHP waiting module.

### 6.2 Security level evaluation of the countermeasure module

To evaluate the security level of the proposed approach, a simulation model is developed. In the sequel, the implemented simulation model is presented and the obtained numerical results for evaluating our proposal are explored. Therefore, the simulation model is developed by randomly generating

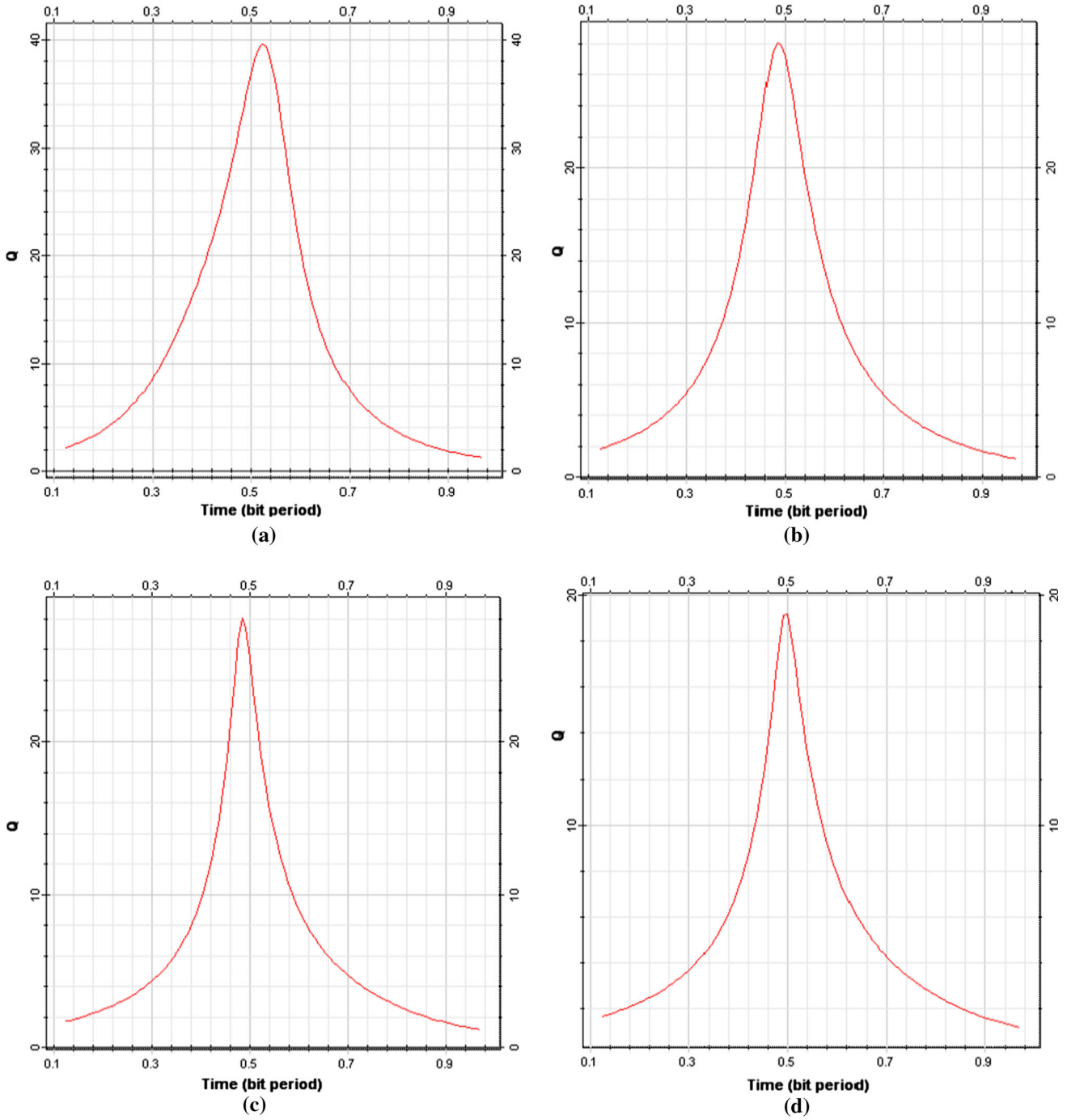


**Fig. 13** Q factor curves for different filtering overheads, **a** filtering delay: 5 tours, **b** filtering delay: 8 tours, **c** filtering delay: 10 tours, **d** filtering delay: 12 tours

a meshed network. Traffic demand between two edge nodes is randomly chosen from the interval [0,1] using uniform distribution. The security level of the proposed approach is evaluated in terms of burst blocking probability and average delay. This is done by generating bursts according to a Poisson distribution with a mean arrival rate $\lambda$ and an exponentially distribution length with a mean $\mu$. The traffic load is defined as $\rho = \frac{\lambda}{\mu}$. For each physical link, this traffic load is the cumulative load of all-optical paths that flow through it. In addition, we consider a BHP erroneous load relatively to the total load on a physical link.

In order to analyze the security efficiency of the proposed countermeasure module, we focus on testing the variation effect of the following parameters:

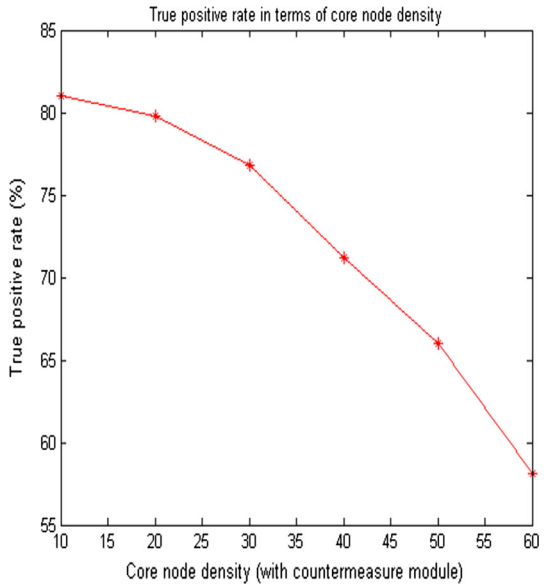


**Fig. 14** True positive rate in terms of core node density

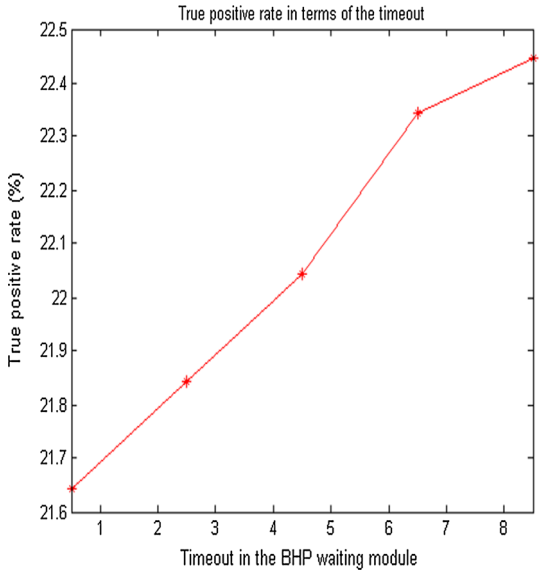


**Fig. 15** True positive rate in terms of the timeout

- The average number of the optical buffers (BHP waiting modules) per core node that implements the countermeasure module.
- The density of the core nodes that implement the countermeasure module in the network.
- The timeout (buffering delay) in the BHP waiting module.

Figure 14 depicts the effect of the core node density (core nodes that implement the countermeasure module) on the true positive rate. A true positive refers to the case where a malicious BHP is correctly dropped by the countermeasure module. We notice that the true positive rate increases when the core node density in the OBS network increases. Thus, the detection of erroneous and legitimate BHPs can be assured only by nodes that implement the BHP flooding countermeasure module. Therefore, the variation of the core node density in the network has a critical effect on the global security level performance in the network.

Furthermore, Fig. 15 describes the effect of the timeout, which corresponds to the maximal buffering delay in the BHP waiting module, on the true positives. A true positive refers to the case when an erroneous BHP is correctly detected and dropped due to the reception of a duplicated copy of the same BHP before the timeout elapse in the waiting module. We can notice that the true positive rate increases when the timeout increases. Thus, the choice of the timeout is critical on the global network performances and must maximize the true positive rate in the network. However, the increase in the timeout can lead to the drop of legitimate BHPs due to their quality degradation in the VOM.

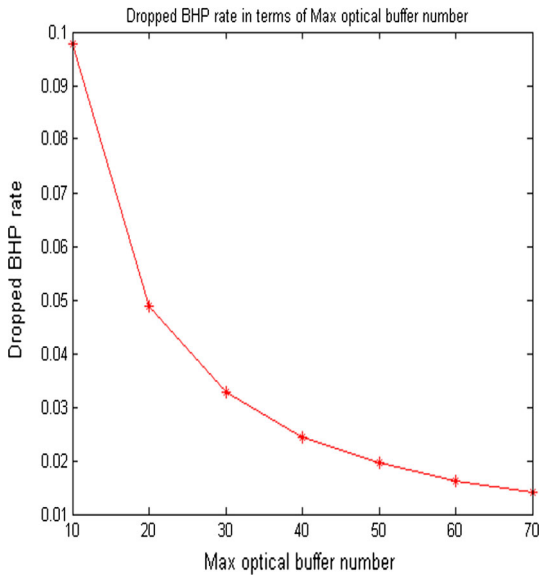


**Fig. 16** Dropped BHP rate in terms of optical buffer number

Figure 16 describes the dropped BHP rate as a function of VOM capacity (number of available optical buffers) per core node. We can notice that the dropped BHP rate decreases when the optical buffer number per core node increases. Indeed, a control packet may arrive when there is no available optical buffer, and it will be dropped by the proposed countermeasure module. This affects the correctness property of the proposed approach that requires to filter correctly the traffic that must be filtered. Therefore, better performances could be obtained by increasing the number of available optical buffers per core node.

## 7 Conclusion

OBS networks are subject to several novel attacks that should be classified. Among these attacks, several DoS attacks can be studied and investigated (DoS attack based on the modification of codewords, Burst replay, etc). This raises the need to develop a minimal number of optical circuits that should be reconfigurable to detect a maximal number of attacks.

In the frame of this work, we have studied a new category of attacks that aims at exhausting the capabilities of core nodes by flooding a core node with huge number of fake control packets. Furthermore, we have proposed a reconfigurable countermeasure module based on optical codewords and tunable decoders. The present work includes the first study of the denial of service attack resulting from vulnerabilities in the resource reservation protocols in OBS networks. The proposed countermeasure module performs the fake control packets filtering at the optical layer based on the concept of optical codewords. An optical codeword is associated with a source node address in order to allow the optical layer processing of control packets. The proposed countermeasure module is built using components available by current technology; therefore, it is implementable. We have evaluated the performances of the proposed countermeasure module by assessing its security level and its effect on the signal quality.

## References


[1] Kartalopoulos, S.: Quantum Cryptography for Secure Optical Networks. (Glasgow, Scotland) (2007)

[2] Ghafouri-Shiraz, H., Karbassian, M.M.: Optical CDMA Networks: Principles, Analysis and Applications. Wiley-IEEE Press, Hoboken (2012)

[3] Soriano, M.C., Colet, P., Mirasso, C.R.: Security implications of open- and closed-loop receivers in all-optical chaos-based communications. IEEE Photonics Technol. Lett. **21**, 426–428 (2009)

[4] Marquis, D., Medard, M., Barry, R.A., Finn, S.G.: Security issues in all-optical networks. IEEE Netw. **3**, 42–48 (1997)

[5] Wu, T., Somani, A.K.: Cross-talk attack monitoring and localization in all-optical networks. IEEE/ACM Trans. Netw. **13**, 1390–1401 (2005)

[6] Mas, C., Tomkos, I., Tonguz, O.K.: Failure location algorithm for transparent optical networks. IEEE J. Sel. Areas Commun. **23**, 1508–1519 (2005)

[7] Sivakumar, M., Shenai, R.K., Sivalingam, K.M.: A Survey of Survivability Techniques for Optical WDM Networks. Ch 3. Springer Science, Berlin (2005)

[8] Sun, X., Chan, C.K., Chen, L.K.: A survivable WDM-PON architecture with centralized alternate-path protection switching for traffic restoration. IEEE Photonics Technol. Lett. **18**, 631–633 (2006)

[9] Sun, X., Chan, C.K., Wang, Z., Lin, C., Chen, L.K.: A single-fiber bi-directional WDM self-healing ring network with bi-directional OADM for metro-access applications. IEEE J. Sel. Areas Commun. **5**, 18–24 (2007)

[10] Fok, M., Wang, Z., Deng, Y., Prucnal, P.: Optical layer security in fiber-optic networks. IEEE Trans. Inf. Forensics Secur. **6**, 725–736 (2011)

[11] Yuan, S., Stewart, D.: Protection of optical networks against interchannel eavesdropping and jamming attacks. In: International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, pp. 34–38, 10–13 March 2014

[12] Chen, Y., Verma, P. K.: Secure optical burst switching: framework and research directions. In: IEEE Communication Magazine, Aug 2008

[13] Chen, Y., Verma, P.K., Kak, S.: Embedded security framework for integrated classical and quantum cryptography services in optical burst switching networks. Secur. Commun. Netw. **2**, 546–554 (2009)

[14] Subramanian, P.S., Muthuraj, K.: Threats in optical burst switched network. Int. J. Comput. Technol. Appl. **2**, 510–514 (2011)

[15] Furdek, M., Skorin-Kapov, N.: Physical-layer attacks in all-optical WDM networks. In: Proceedings of the 34th International Convention, Opatija, Croatia, May 2011

[16] Skorin-Kapov, N., Chen, J., Wosinska, L.: A new approach to optical networks security: attack-aware routing and wavelength assignment. IEEE/ACM Trans. Netw. **18**(3), 750–760 (2010)

[17] Furdek, M., Skorin-Kapov, N., Zsigmond, S., Wosinska, L.: Vulnerabilities and security issues in optical networks. In: 16th International Conference on Transparent Optical Networks (ICTON), Graz, Austria, pp. 1–4, 6–10 July 2014

[18] Sliti, M., Hamdi, M., Boudriga, N.: A novel optical firewall architecture for burst switched networks. In: Proceedings of the 12th International Conference on Transparent Optical Networks (ICTON 2010) (2010)

[19] Muthuraj, K., Sreenath, N.: Secure optical internet: an attack on OBS node in a TCP over OBS network. Int. J. Emerg. Trends Technol. Comput. Sci. **1**(4), 75–80 (2012)

[20] Batti, S., Zghal, M., Boudriga, N.: New all-optical switching node including virtual memory and synchronizer. J. Netw. **5**, 165–179 (2010)

[21] Pradeep, C.: Implementation of optical burst switched IP-over-WDM networks using tunable transmitter and tunable receiver. In: Proceedings of the International Conference on Communication Systems and Network Technologies, Gwalior, India, April 2013

[22] Li, H., Yin., H.: An analytical approach to chaotic behavior of TCP in OBS networks. In: Proceedings of the International Conference on Communications in China, Xi'an, China, Aug 2013

[23] Riadi, S., Ghanami, D.E., Maach, A.: An efficient burst cloning scheme for optical burst switching over star networks. In: Proceedings of the ACS International Conference on Computer Systems and Applications, Ifrane, Morocco, May 2013

[24] Coulibaly, Y., Latiff, M., Selamat, A.: A novel routing optimization in optical burst switching networks. In: Proceedings of the Second International Conference on Communication Theory, Reliability, and Quality of Service, Colmar, France, July 2009

[25] Djordjevic, I.B., Vasic, B.V.: Novel combinatorial construction of optical orthogonal codes for incoherent optical CDMA system. J. Lightwave Technol. **21**, 1869–1875 (2003)

[26] Boudriga, N., Sliti, M., Abdallah, W.: Optical code-based filtering architecture for providing access control to all-optical networks. In: Proceedings of International Conference on Transparent Optical Networks (ICTON 2012), (2012)

[27] Liu, Y., Hill, M., de Waardt, H., Khoe, G., Dorren, H.: All-optical buffering using laser neural networks. IEEE Photonics Technol. Lett. **15**, 596–598 (2003)

[28] Guan, Y., Wang, R.: Demonstration of an optical switch based on SOA-MZI operation at 10 gbit/s. In: Proceedings of the International Conference on Artificial Intelligence and Software Engineering, China, July 2013

[29] Rostam, R., Wahid, M., Rais, S., Faridus, M.: The effect of signal repetition rate, injected current and switching window on cross-phase modulation in SOA-NOLM. In: Proceedings of the IEEE Regional Symposium on Micro and Nanoelectronics, Malaysia, Sept 2011

[30] Tan, H.N., Matsuura, M., Kishi, N.: Parallel WDM regenerative waveform conversion for mixed NRZ and RZ transmission networks using a SOA-based multiple switching-window optical gate. In: Proceedings of the Optical Fiber Communication Conference and Exposition (OFC/NFOEC), Los Angeles, USA, March 2011

**Maha Sliti** received her Engineer Diploma in Telecommunications and Computing Networks from the National Institute of Applied Sciences and Technology (INSAT) at the University of Carthage, Tunisia, her MS degree in Telecommunications from the Engineering School of Communication of Tunis (SUP'COM) at the University of Carthage, Tunisia, and her Ph.D. degree in Telecommunications at SUP'COM. Since November 2011, she has been working as an assistant at Higher Institute of Computer and Communication Techniques (ISITCOM). She is also affiliated with the Communication Networks and Security (CN&S) Laboratory at SUP'COM, where she is conducting research work in the areas of security and routing in all-optical networks.

**Noureddine Boudriga** is an internationally known scientist/academic. He received his Ph.D. in Algebraic topology from University Paris XI (France) and his Ph.D. in Computer science from University of Tunis (Tunisia). He is currently a Professor of Telecommunications at University of Carthage, Tunisia and the Director of the Communication Networks and Security Research Laboratory (CNAS). He has served as the General Director and founder of the Tunisian National Digital Certification Agency. He was involved in very active research and authored or coauthored many chapters and books. He published over 250 refereed journal and conference papers. Prof. Boudriga is the President of the Tunisia Scientific Telecommunications Society. He is the recipient of the Tunisian Presidential award in Science and Research (2004).